Letter

A Novel Dynamic Watermarking-Based EKF Detection Method for FDIAs in Smart Grid

Xue Li, Ziyi Wang, Changda Zhang, Dajun Du, and Minrui Fei

Dear editor,

The existing bad data detection (BDD) cannot effectively detect false data injection attacks (FDIAs) in smart grid. The objectiveness of this letter is to investigate a novel dynamic watermarking (DW)-based extended Kalman filter (EKF) detection method to detect FDIAs. Firstly, security weakness of traditional χ^2 detector is analyzed, and a novel DW-based EKF detection method is proposed for FDIAs. Secondly, the detection effectiveness and security property of the proposed method are analyzed theoretically, where not only the positive correlation between the detection performance and DW signal intensity but also zero impact of FDIAs not being detected on smart grid (SG) are revealed. Finally, the effectiveness of the proposed method is confirmed by experimental results.

Related work: With the rapid development of information and new energy technologies, the traditional power system is gradually migrating to SG [1], [2], where wired/wireless communication networks are employed to support the operation and running of SG [3], [4]. However, these communication networks make SG vulnerable to cyber attacks. For cyber attacks in SG, some issues such as attack detection, recovery after attack, security control and so on have been reported [5]. Specially, attack detection methods of rapidly discovering cyber attacks have attracted wide attention from academic and engineering field.

FDIAs are a kind of typical cyber attacks. A successful FDIAs on supervisory control and data acquisition (SCADA) will bring untrue measuring data, which will make state estimator produce wrong data to the operator, affecting seriously safe running of SG [6]. Therefore, it is of great significance to study the detection of FDIAs. When cyber attack signals obey Gaussian distribution, Kalman filter-based χ^2 detection method is usually employed for detection [7]. A data-driven learning-based algorithm is also proposed to detect FDIAs in SG [8].

However, the attacker always tries to bypass attack detection and destroys the stability and economy of SG. Recently, dynamic watermarking [9] has been employed to support attack detection and secure control. Therefore, inspired by the idea of DW, this letter will investigate new DW-based attack detection method for FDIAs, but there exist the following challenges: How to design a new DW-based detection method against FDIAs? What are detection effectiveness and security property of the proposed new detection method?

To solve these challenges, this letter proposes a new DW-based EKF detection method for FDIAs in SG. Compared with the existing methods in the literatures, comparative analysis is listed in Table 1. It can be clearly seen that security weakness of traditional χ^2-based detector is analyzed while detection performance and security property of the proposed new DW-based EKF detection method are proved.

Corresponding author: Ziyi Wang.

Citation: X. Li, Z. Y. Wang, C. D. Zhang, D. J. Du, and M. R. Fei, "A novel dynamic watermarking-based EKF detection method for FDIAs in smart grid," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 7, pp. 1319–1322, Jul. 2022.

The authors are with Shanghai Key Laboratory of Power Station Automation Technology, the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444, China (e-mail: lixue@shu.edu.cn; suntai@shu.edu.cn; changdazhang@shu.edu.cn; ddj@i.shu.edu.cn; mrfei@staff.shu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2022.105704

Table 1. Comparative Analysis Between the Proposed Method and Existing Methods

	System	DM	DT	SW of TD	SP	DP
[7]	Linear	KF	χ^2 detection	×	×	×
[10]	Linear	DW	KL-divergence	×	×	√
Proposed method	Nonlinear	DW	Consistent tests	√	√	√

DM: Detection mechanism; DT: Detection test
SW of TD: Security weakness of traditional χ^2-based detector
SP: Security property; DP: Detection performance

Problem statement:

1) AC model of SG: The dynamic operation of AC power grid can be described approximately by a continuous state-space model, which includes the following state and measurement equations:

$$x(k+1) = f(x(k)) + \delta(k) \tag{1}$$

$$z(k) = h(x(k)) + \upsilon(k) \tag{2}$$

where $x(k) \in \mathbb{R}^n$ are system state including voltage magnitude V and voltage angle θ, $z(k) \in \mathbb{R}^m$ are system measurements including node active injection power P_i, node reactive injection power Q_i, branch active power flow P_{ij}, branch reactive power flow Q_{ij}, $f(x(k))$ and $h(x(k))$ are nonlinear state transfer function and nonlinear measurement function based on Ohm's and Kirchhoff's laws, $\delta(k) \in \mathbb{R}^n$ and $\upsilon(k) \in \mathbb{R}^m$ are independent identically distributed (i.i.d.) zero mean white Gaussian with covariance matrices Σ_δ and Σ_υ, respectively.

Remark 1: Since it is difficult to obtain the concrete form of $f(x(k))$ [11], the popular Holt's two parameter exponential smoothing method are used to identify $f(x(k))$. With Kirchhoff's voltage law and other circuit theorems, $h(x(k))$ can be expressed as

$$\begin{aligned}
P_i &= \textstyle\sum_{j=1}^{N} V_i V_j \left(G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}\right) \\
Q_i &= \textstyle\sum_{j=1}^{N} V_i V_j (G_{ij}\sin\theta_{ij} - B_{ij}\cos\theta_{ij}) \\
P_{ij} &= V_i^2 g - V_i V_j g\cos\theta_{ij} - V_i V_j b\sin\theta_{ij} \\
Q_{ij} &= -V_i^2 (b + y_c) - V_i V_j g\sin\theta_{ij} + V_i V_j b\cos\theta_{ij}
\end{aligned}$$

where i and j are the serial number of nodes, $\theta_{ij} = \theta_i - \theta_j$ represents the voltage phase difference, G_{ij} and B_{ij} represent the conductance and susceptance, g, b and y_c represent line conductance, line susceptance and line to ground admittance of the branch, respectively.

2) EKF under FDIAs and χ^2 detector: Since SG under normal conditions is known as quasi-stationary regime, i.e., the system experiences change smoothly and slowly [12], it can be linearized at about an operating point in the framework of EKF with high accuracy. Thus, using parameter identification and Taylor expansion, (1) and (2) can be linearized as

$$x(k+1) = Fx(k) + G(k) + \delta(k) \tag{3}$$

$$z(k) = Hx(k) + \upsilon(k) \tag{4}$$

where F is state transition matrix, $G(k)$ is state vector, $H \in \mathbb{R}^{m\times n}$ represents Jacobian matrix of $h(x(k))$.

Remark 2: The Holt's two parameter exponential smoothing method can be used to calculate F and $G(k)$ in (3), and it follows that:

$$\begin{aligned}
F &= \alpha(1+\beta)I \\
G(k) &= (1+\beta)(1+\alpha)\tilde{x}(k|k-1) \\
&\quad -\beta a(k-1) + (1-\beta)b(k-1)
\end{aligned}$$

where two variables $a(k) = \alpha\hat{x}(k|k) + (1+\alpha)\tilde{x}(k|k-1)$ and $b(k) = \beta(a(k) - a(k-1)) + (1-\beta)b(k-1)$, $\tilde{x}(k|k-1)$ is the predicted value and $\hat{x}(k|k)$ is the estimated value.

When $z(k)$ is attacked by FDIAs, the typical FDIAs commonly adopt scaling, injection, replacement, and so forth [13]. Here, we consider the FDIA with scaling and injection, i.e.,

$$z^a(k) = z(k) + \Gamma z(k), \quad k \in [k_0^a, \infty) \tag{5}$$

where k_0^a is the initial instant attacked by FDIAs, $\Gamma \in \mathbb{R}^{m\times m}$ is the

attack matrix, e.g., Γ is defined by a diagonal matrix

$$[\Gamma]_{ii} = \begin{cases} \gamma, & \text{for some } i \\ 0, & \text{otherwise} \end{cases}$$

where $\gamma = (z_i^a - z_i)/z_i$ is attack intensity for the ith attacked element (i.e., z_i with $[\Gamma]_{ii} = \gamma$).

Next, for (3)–(5), a steady-state EKF is used to estimate state of SG. Refer to EKF without attack [14], $\tilde{x}(k|k-1)$ and the estimated value $\hat{x}(k|k)$ under FDIAs can be expressed as

$$\tilde{x}(k|k-1) = Fx(k-1) + G(k) \tag{6}$$

$$\hat{x}(k|k) = \tilde{x}(k|k-1) + K(z^a(k) - H\tilde{x}(k|k-1)) \tag{7}$$

where $\bar{e}(k) = z^a(k) - H\tilde{x}(k|k-1)$ is the residual under FDIAs, $K = PH^T(HPH^T + \Sigma_v)^{-1}$ is Kalman gain, P is steady-state prediction error covariance without attack.

To detect cyber attacks, χ^2 detector is commonly used, i.e.,

$$\lambda(k) = \bar{e}^T(k)\Sigma_{e^0}^{-1}\bar{e}(k) \tag{8}$$

where $\Sigma_{e^0} = HPH^T + \Sigma_v$ is the covariance of the residual $\bar{e}(k)$ without attack.

3) Security weaknesses analysis of χ^2 detector: Security weaknesses of χ^2 detector will be analyzed with the help of system residual and its covariance. When SG suffers from FDIAs, the residual $\bar{e}(k)$ becomes as

$$\bar{e}(k) = \tilde{e}(k) + \Gamma z(k) \tag{9}$$

where $\tilde{e}(k) = z(k) - H\tilde{x}(k|k-1)$. Furthermore, the residual covariance can be written as

$$E[\bar{e}(k)\bar{e}^T(k)] = E[\tilde{e}(k)\tilde{e}^T(k)] + \Gamma E[z(k)z^T(k)]\Gamma^T + 2E[\tilde{e}(k)z^T(k)]\Gamma^T. \tag{10}$$

When Γ is small, $\bar{e}(k)$ and its covariance are approximately equal to those of attack-free system, respectively. According to the setting of χ^2 detection, it is easy to know that when Γ is small, there is little difference between χ^2 detection value of the attacked system and that of the attack-free system. It means that the traditional χ^2 detector cannot effectively detect FDIAs.

New dynamic watermarking-based EKF detection method for FDIAs in smart grid: To overcome security weakness of the traditional χ^2 detector, DW is used to protect the measurement fed back to state estimator [10]. Thus, a new DW-based EKF detection method is proposed for SG under FDIAs. Meanwhile, the detection performance and security property of the detector will also be discussed.

1) A new DW-based EKF detection method for FDIAs: The framework of new DW-based EKF detection method for FDIAs in SG is shown in Fig.1. The measurement $z(k)$ is firstly sampled, which is then encrypted by watermarking signal $w(k)$ (i.e., as a key), becoming $z_w^+(k)$. If $z_w^+(k)$ is attacked and becomes $z^a(k)$, it is decrypted with $w(k)$ and saved as $z_w^-(k)$. Furthermore, using $z_w^-(k)$, $w(k)$ and $\tilde{x}(k|k-1)$, attack detector can check whether or not $z_w^-(k)$ is attacked.

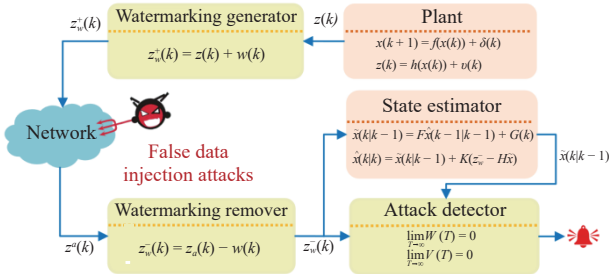

Fig. 1. DW-based EKF detection for FDIAs in smart grid.

For (3) and (4), to guarantee data security, $z(k)$ is encrypted by watermarking, i.e.,

$$z_w^+(k) = z(k) + w(k) \tag{11}$$

where $w(k)$ is DW signal (i.e., an i.i.d. Gaussian random variable with zero mean and covariance Σ_w), and it is independent of $z(k)$. Then, $z_w^+(k)$ is transmitted through the network to state estimator, if it is attacked and then becomes $z^a(k)$. Therefore, $z^a(k)$ in (5) can be re-written as

$$z^a(k) = z_w^+(k) + \Gamma z_w^+(k), \quad k \in [k_0^a, \infty). \tag{12}$$

Next, using watermarking remover, $z^a(k)$ becomes as

$$z_w^-(k) = z^a(k) - w(k). \tag{13}$$

Furthermore, $z_w^-(k)$ will be sent to the state estimator, and (6) and (7) can be re-written as

$$\tilde{x}(k|k-1) = Fx(k-1) + G(k) \tag{14}$$

$$\hat{x}(k|k) = \tilde{x}(k|k-1) + K\left(z_w^-(k) - H\tilde{x}(k|k-1)\right). \tag{15}$$

Here, the residual can be redefined as $e(k) = z_w^-(k) - H\tilde{x}(k|k-1)$.

Next, $z_w^-(k)$ is transferred to attack detector which will be employed to check whether or not SG is attacked by the following two tests.

Test 1: Check if

$$\lim_{T\to\infty} W(T) = 0 \tag{16}$$

where $W(T) = (1/T)\sum_{k=1}^{T} Ke(k)(Ke(k))^T - K\Sigma_{e^0}K^T$, T is the time window size.

Test 2: Check if

$$\lim_{T\to\infty} V(T) = 0 \tag{17}$$

where $V(T) = (1/T)\sum_{k=1}^{T} w(k)(Ke(k))^T$.

To detect FDIAs, Tests 1 and 2 must be converted to the statistical tests $\rho_1(k) = |\mathrm{tr}W^k(T)|$ and $\rho_2(k) = \|V^k(T)\|$ for practical applications, where $W^k(T)$ and $V^k(T)$ are $W(T)$ and $V(T)$ within the current time window $\{k-T+1, k-T+2, \ldots, k\}$, respectively. Furthermore, let ζ_1 and ζ_2 be the preset thresholds and if $z_w^-(k)$ is attacked, $\rho_1 \geq \zeta_1$ or $\rho_2 \geq \zeta_2$ is expected. An online detection procedure is given by the following Algorithm 1.

Remark 3: Note that to prevent measurement noise and disturbance input being regarded as bad data (i.e., causing false alarm), the thresholds ζ_1 and ζ_2 should be selected bigger than maximal attack-free tests ρ_1 and ρ_2, respectively.

Algorithm 1 Online Detection Algorithm for FDIAs

```
Initialization: Set threshold ζ1 and ζ2,
while k = T, T+1, ... do
  Obtain the values of w(k), z_w^-(k), x̃(k|k-1)
  Σ_t1 ← 0, Σ_t2 ← 0
  while j = k-T+1, k-T+2, ..., k do
    Compute
      e(k-j) = z_w^-(k-j) - Hx̃(k-j|k-j-1)
    Σ_t1 ← Σ_t1 + Ke(k-j)(Ke(k-j))^T
    Σ_t2 ← Σ_t2 + w(k-j)(Ke(k-j))^T
  end
  Compute W^k(T) = (1/T)Σ_t1 - KΣ_e0 K^T and V^k(T) = (1/T)Σ_t2
  Obtain ρ1(k) and ρ2(k)
  if ρ1 ≥ ζ1 ∨ ρ2 ≥ ζ2 then
    Claim attacks
  end
end
```

2) Detection effectiveness analysis of new DW-based EKF detection method for FDIAs: The detection performance of the proposed detection method will be presented by the following Theorem 1.

Theorem 1: For the system in (3), (4) and (11)–(15), FDIAs will result in

$$E[e^T(k)e(k)] = E[\tilde{e}(k)\tilde{e}^T(k)] + \Gamma E[z(k)z^T(k)]\Gamma^T + 2E[\tilde{e}(k)z^T(k)]\Gamma^T + \Gamma\Sigma_w\Gamma^T \tag{18}$$

$$E[w(k)e^T(k)] = \Sigma_w\Gamma^T. \tag{19}$$

Proof: Due to the existence of $w(k)$, $e(k)$ can be re-written as $e(k) = (1+\Gamma)z(k) - H\tilde{x}(k|k-1) + \Gamma w(k)$. With the help of the above formula, the covariance of $e(k)$ can be obtained in (18). Taking the

covariance of $e(k)$ and $w(k)$ and considering $w(k) \perp \tilde{x}(k|k-1)$ and $w(k) \perp z(k)$ leads to (19). ■

Remark 4: When no attack occurs (Γ is zero matrix), the last three terms of (18) and the right side of (19) are 0, and DW tests are satisfied. When FDIAs occur, the above does not hold, DW tests are not satisfied, FDIAs are detected. Even Γ is small, different from χ^2 detector, Σ_w can be increased to ensure that DW-based EKF detector can detect FDIAs. Moreover, the positive correlation between the detection effectiveness of DW-based EKF detector and the watermarking intensity is also revealed by (18) and (19). With the increasing of watermarking intensity Σ_w, cross covariance of watermarking and the residuals and auto-covariance of the residuals increase, which means $W(T)$ and $V(T)$ enlarge. Thus, it improves the detection effectiveness of DW-based EKF detector.

3) Security property analysis of new DW-based EKF detection method for FDIAs: The detection effectiveness of DW-based EKF detection method has been analyzed. When the attacks bypass the detector, security performance is then analyzed. To quantify the additional distortion caused by FDIAs, it is defined as

$$D_e(k) = Ke(k) - Ke^0(k). \tag{20}$$

According to $\{D_e\}$, the additive distortion power [9] is defined by $\lim sup_{T\to\infty}(1/T)\sum_{k=1}^{T}\|D_e(k)\|^2$. Then, security property is analyzed by the following Theorem 2.

Theorem 2: For the system in (3), (4) and (11)–(15), $z_w^-(k)$ passes Tests 1 and 2, then

$$\lim_{T\to\infty}\sup\frac{1}{T}\sum_{k=1}^{T}\|D_e(k)\|^2 = 0. \tag{21}$$

It means that when the FDIAs (12) bypass Tests 1 and 2, the additional distortion power of the system is limited to 0.

Proof: Since $z_w^-(k)$ passes Tests 1 and 2, by analyzing security property, it follows that:

$$\lim_{T\to\infty}\frac{1}{T}\sum_{k=1}^{T}D_{e,i}(k)D_{e,j}(k) + D_{e,i}(k)[K_{j.}e^0(k)] \times D_{e,j}(k)[K_{i.}e^0(k)] = 0 \tag{22}$$

$$\lim_{T\to\infty}\frac{1}{T}\sum_{k=1}^{T}w_i(k)D_e^T(k) = 0. \tag{23}$$

According to (6) and (7), the residual of the attack-free system can be given by

$$e^0(k) = -HF\hat{x}^0(k-1|k-1) - HG^0(k) + z_w^{0-}(k). \tag{24}$$

Defining $e_{K,i}^0(k) := K_{i.}e^0(k)$ and using Martingale stability theorem, we have

$$\sum_{k=1}^{T}D_{e,i}(k)e_{K,i}^0(k) = o\left(\sum_{k=1}^{T}D_{e,i}^2(k)\right) + O(1). \tag{25}$$

Substituting (25) into (22) yields

$$\sum_{k=1}^{T}D_{e,i}^2(k) + 2D_{e,i}(k)[K_{i.}e^0(k)] = (1+o(1))\sum_{k=1}^{T}D_{e,i}^2(k) + O(1). \tag{26}$$

Diving (26) by T and taking its limit as $T\to\infty$, it can be obtained

$$\lim_{T\to\infty}\frac{1}{T}\sum_{k=1}^{T}D_{e,i}^2(k) = 0, \quad i = 1,2,...,n. \tag{27}$$

Considering $\|D_e(k)\| = \sqrt{\sum_{i=1}^{n}D_{e,i}^2}$, (21) can be obtained by (27). ■

Remark 5: Theorem 2 reveals that when FDIAs with very small attack intensity bypass DW Tests 1 and 2, the additive distortion power is restricted to be zero and the impact on SG can be ignored. Moreover, it indicates that theoretical basis of attack detection is (21).

Experiments: IEEE 14-bus system is employed to validate the proposed method, as shown in Fig. 2. Holt's technique initializes

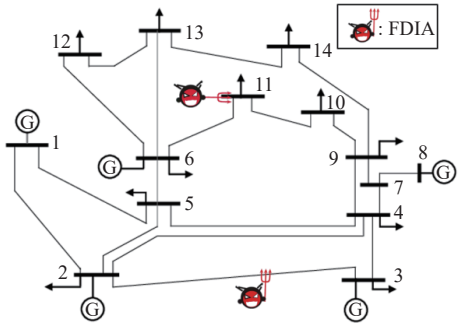

Fig. 2. Schematic diagram of IEEE 14-bus system under FDIAs.

system state with the help of the first two time samples (i.e., $k=0$ and $k=1$) derived from power flow (PF) calculations, and the parameters are set as $\alpha = 0.8$ and $\beta = 0.5$. Then, state estimation based on EKF is operated from $k=2$. Diagonal elements of F_0 and P_0 are set as 1.0 and 1×10^{-6}, respectively.

FDIAs in (5) emerge at $k \geq 3$ and

$$\Gamma = \text{diag}\{0,0,1,1,1,0,1,1,0,0,0,1,1,0,1,0,1,0,0,0, 0,0,0,1,1,0,0,1,1,1,1,1,0,0,1,0,1,0,1,0,0,1,0,0, 0,1,0,0,0,1,1,1,0,1,1,0,1,0,1,1,1,0,0,1\}\gamma$$

where attack intensity $\gamma = (z_i^a - z_i)/z_i$ is a constant.

DW signal covariance $\Sigma_w = 4\times10^{-2}$ is set and the time window size is set as $T=20$. The detection thresholds for DW-based EKF method are set as $\zeta_1 = 6\times10^{-4}$ and $\zeta_2 = 3\times10^{-2}$.

Fig. 3 shows the detection results of χ^2 detector and DW-based EKF detector under the same FDIAs. Obviously, χ^2 detector cannot detect FDIAs at all. The strong robustness of SG ensures the stable operation of SG will not be affected by short-term FDIAs. However, as FDIAs continue to destroy measurement data, the stability of SG is destroyed. The influence of FDIAs on data is marked and amplified by DW, which ensures that DW-based EKF detector can detect FDIAs quickly and sensitively. Moreover, when DW signal is too weak to mark attacked data effectively, FDIAs possibly bypass DW-based EKF detector, resulting in misdetection. Due to page limit, the corresponding results are not presented. Therefore, DW-based EKF detector also need to choose appropriate DW signal.

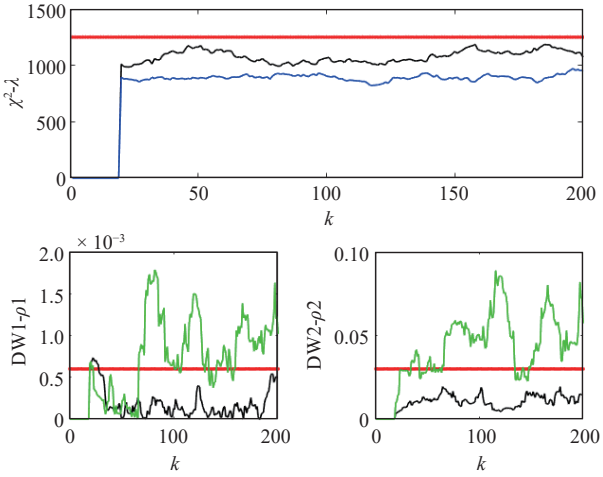

Fig. 3. Comparison of detection results between χ^2 detector and the proposed DW-based EKF method. Black line: Normal system. Blue line: System under the FDIAs without watermarking. Green line: System under the FDIAs with watermarking. Red line: Detection threshold. The detection threshold of χ^2 detector is $\zeta_3 = 1250$, which is based on the principle of ensuring no false detection without attack.

Additional distortion power of SG under different attack intensities is shown in Fig. 4. With the increase of attack intensity γ, the system additive distortion power increases gradually. When the attack

intensity is only $\gamma = -0.2$, the additive distortion power of the system is very close to that of the attack-free system (i.e., $\gamma = 0$). It also means that DW-based EKF detector cannot detect the FDIAs with this intensity.

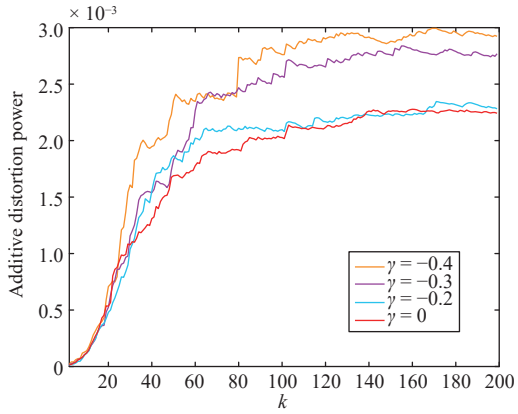

Fig. 4. Additive distortion power under different intensity attacks.

To analyze the impact of FDIAs on SG at attack intensity $\gamma = -0.2$, considering that the system operates close to the upper power limit of transmission line, the upper power limits of 1–3 transmission lines are 100 MW, 50 MW and 50 MW, respectively, and the upper power limits of other transmission lines are 40 MW.

Table 2 shows the optimal power flow (OPF) calculation results before and after FDIAs. Compared with the original optimal power flow calculation results, it shows that there is little change of the optimal power flow operation cost of the system before and after FDIAs with $\gamma = -0.2$, and the system is not affected in general. However, the state estimation results after FDIAs change load distribution and power flow of the system, which finally leads to the adjustment of power generation distribution.

Table 2. Optimal Power Flow Results Before and After Attacks

		OPF before attack		OPF after attack	
		P (MW)	Q (MVar)	P (MW)	Q (MVar)
Generation power distribution	1	149.65	0.06	149.69	0.00
	2	36.61	17.44	36.68	15.83
	3	36.41	23.45	35.81	232.24
	6	9.04	6.73	11.42	8.92
	8	33.20	6.75	30.76	5.16
Total generating power		264.90	54.90	264.36	53.15
Running cost ($/h)		8194.78		8170.90	

According to power flow calculation of the system, Table 3 shows the power flow calculation results before and after FDIAs of some corresponding transmission branches. Since there are many transmission branches, only 5 transmission branches that are more prone to overload are analyzed including transmission branches 1-2, 1-5, 2-3, 2-4 and 4-5. In comparison with the power flow results before and after FDIAs in Table 3, it is not difficult to see that FDIAs with $\gamma = -0.2$ has little impact on SG power flow, but it will still lead to the adjustment of branch power flow.

Conclusions: This letter has proposed a new DW-based EKF detection method for FDIAs in SG. Security weaknesses of χ^2 detector is firstly analyzed and a new DW-based EKF detection method for FDIAs is presented by integrating the watermarking as symmetric-key encryption and DW tests. Using cross covariance of watermarking and the residuals and auto-covariance of the residuals, the positive correlation between the detection effectiveness of FDIAs and the watermarking intensity has then been proved. Furthermore, additional distortion power of the system has been provided to demonstrate security property of the proposed method. Finally, the effectiveness of the proposed method is confirmed on IEEE 14-bus system. However, according to the proposed DW-based EKF detection results, the recovery and security control of SG under FDIAs are interesting future research direction.

Table 3. Power Flow Results Before and After Attacks

Transmission line	PF before attack		PF after attack	
	P (MW)	Q (MVar)	P (MW)	Q (MVar)
1-2	156.88	−20.40	156.30	−20.27
1-5	75.51	3.85	75.43	3.55
2-3	73.24	3.56	73.00	3.58
2-4	56.13	−1.55	55.79	−2.27
4-5	−61.16	15.82	−59.66	17.03

Acknowledgments: The work was supported in part by the National Science Foundation of China (92067106, 61773253, 61803252, 61833011), and Project of Science and Technology Commission of Shanghai Municipality (20JC1414000, 19510750300, 21190780300).

References

[1] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 176–190, 2021.

[2] X. Ge, Q.-L. Han, L. Ding, Y.-L. Wang, and X.-M. Zhang, "Dynamic event-triggered distributed coordination control and its applications: A survey of trends and techniques," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 50, no. 9, pp. 3112–3125, 2020.

[3] X. Zhang, Q.-L. Han, X. Ge, D. Ding, L. Ding, D. Yue, and C. Peng, "Networked control systems: A survey of trends and techniques," *IEEE/CAA J. Autom. Sinica.*, vol. 7, no. 1, pp. 1–17, 2020.

[4] X. Li, C. Jiang, D. Du, R. Wang, M. Fei, X. Li, and Y. Tian, "Optimization and control of cyber–physical power systems under dual-network interactive cascading failure," *Control Engineering Practice*, vol. 111, p. 104789, 2021, DOI: 10.1016/j.conengprac.2021.104789.

[5] D. Du, X. Li, W. Li, R. Chen, M. Fei, and L. Wu, "ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1698–1711, 2019.

[6] 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, 2020.

[7] J. Cheng, X. Sun, P. Liu, and H. Mou, "An improved residual Chi-square test fault isolation approach in four-gyro SINS," *IEEE Access*, vol. 7, pp. 174400–174411, 2019.

[8] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, 2021.

[9] D. Du, C. Zhang, X. Li, M. Fei, T. Yang, and H. Zhou, "Secure control of networked control systems using dynamic watermarking," *IEEE Trans. Cybern.*, 2021. DOI: 10.1109/TCYB.2021.3110402.

[10] D. Wang, J. Huang, Y. Tang, and F. Li, "A watermarking strategy against linear deception attacks on remote state estimation under K-L divergence," *IEEE Trans. Ind. Inf.*, vol. 17, no. 5, pp. 3273–3281, 2021.

[11] A. S. Debs and R. E. Larson, "A dynamic estimator for tracking the state of a power system," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-89, no. 7, pp. 1670–1678, Sept. 1970.

[12] A. M. Leita Da Silva, M. B. Do Coutto Filho, and J. F. de Queiroz, "State forecasting in electric power systems," *IEE Proceedings–Generation, Transmission and Distribution*, vol. 130, no. 5, pp. 237–244, Sept. 1983.

[13] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Trans. Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554–1569, Aug. 2019.

[14] C. Muscas, P. A. Pegoraro, S. Sulis, M. Pau, F. Ponci, and A. Monti, "New Kalman filter approach exploiting frequency knowledge for accurate PMU-based power system state estimation," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 9, pp. 6713–6722, 2020.