

Article

Resilient Lyapunov-Based Model Predictive Control for Wind Power System Under False Data Injection Attacks

Ningchen Luo * and Langwen Zhang 

School of Automation Science and Engineering, South China University of Technology, Guangzhou 510641, China; aulwzhang@scut.edu.cn

* Correspondence: 202330461292@mail.scut.edu.cn

Abstract

Wind power systems operating in networked environments are vulnerable to stochastic disturbances, measurement noise, model mismatch and false data injection (FDI) attacks. These uncertainties may corrupt feedback information and degrade closed-loop control performance. This paper proposes an integrated extended Kalman filter (EKF)-based resilient Lyapunov model predictive control (RLMPC) framework for the secure control of wind power systems under bounded stochastic FDI attacks. A residual-based chi-square (χ^2) detector is embedded into the EKF update to evaluate the credibility of received measurements, and the resulting attack-aware state estimate is applied to the RLMPC controller at each sampling instant, constructing an EKF-RLMPC strategy. The proposed EKF-RLMPC scheme therefore links attack detection, state estimation, and predictive control within a unified secure-control framework for wind power systems. It is proved that the posterior estimation error remains bounded and that the closed-loop state is ultimately bounded under the proposed EKF-RLMPC scheme. Simulation studies under different FDI attack probabilities show that the proposed method improves state-estimation accuracy and control performance.

Keywords: wind power system; false data injection attack; extended Kalman filter; chi-square detection; resilient model predictive control

MSC: 93B45

1. Introduction

Wind generation has become an important part of modern renewable-energy systems. However, the control of wind power systems remains challenging because aerodynamic conversion, drivetrain coupling, actuator constraints and wind-speed variability interact over different time scales. These nonlinear and stochastic characteristics make the plant sensitive to modeling uncertainty, random wind fluctuations, and measurement imperfections. Consequently, wind power systems require control strategies that can maintain regulation performance while satisfying physical and operational constraints [1].

The increasing use of communication networks and supervisory automation has also made predictive control attractive for wind-energy applications. MPC is well suited to this setting because actuator limits, operating constraints, and short-horizon system evolution can be handled in one online optimization problem. This receding-horizon principle has been adopted in wind-power control frameworks [2]. MPC-based designs for PMSG grid-connection systems [3], automatic voltage regulation [4], and nonlinear process control [5]



Academic Editor: Duarte Valério

Received: 26 May 2026

Revised: 19 June 2026

Accepted: 23 June 2026

Published: 28 June 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

have been reported. Resilient MPC has also been extended to systems affected by stochastic disturbances and cyber attacks [6–8]. Nevertheless, many existing predictive controllers still update the control input from raw measurements or directly available states. When the sensor-to-estimator channel is compromised, such a design may propagate corrupted information into the optimization problem. Therefore, the trustworthiness of measurements should be assessed before the predictive controller is updated.

Under stochastic disturbances, process and measurement noise introduce uncertainty into the available system-state information and consequently reduce the decision accuracy of the controller [9]. Extended Kalman filtering, unscented Kalman filtering, and observer-based schemes have been widely adopted for state estimation in nonlinear wind power systems [10]. In parallel, H_∞ control, sliding-mode control, and stochastic MPC have been used to enhance robustness against stochastic disturbances [11,12]. More recently, Kalman filtering has been combined with MPC to improve control performance in noisy environments [13,14]. However, most available studies mainly improve estimation or control performance under nonmalicious uncertainty, while the interaction among detection decisions, estimation errors, and constrained predictive optimization under cyber attacks is still not sufficiently characterized.

The integration of communication networks exposes wind power systems to cyber-security threats, including FDI attacks [15–17]. Existing studies on FDI attacks have considered attack modeling, anomaly detection, and secure control. Representative approaches describe attack behavior through stochastic processes [18,19], identify anomalies using residual statistics and chi-square tests [15,16,20], and improve attack resilience by combining secure estimation, Kalman filtering, robust control, adaptive control, and data-driven methods [21–24]. Although these studies provide useful tools, three limitations remain relevant to the present problem. First, attack detection, state estimation, and predictive control are often designed as separated modules, so the resulting closed-loop control law may not explicitly depend on an attack-aware state estimate. Second, many analyses implicitly rely on reliable detection decisions and do not explicitly include false alarms or missed detections in the stability argument. Third, simulation validation is often based on representative trajectories, whereas stochastic FDI attacks require statistical evaluation through repeated trials and baseline comparisons.

To clarify the above gap, Table 1 summarizes the relation between representative research directions and the present work. The comparison is not intended to replace detailed experimental benchmarking; rather, it highlights the methodological components that are simultaneously required for the considered secure wind-power control problem.

Table 1. Comparison between related research directions and the proposed EKF-RLMPC framework.

Research Direction	Stochastic Disturbance	FDI/Security Issue	State Estimator	Residual Detector	Detection-Error Effect	Statistical/Baseline Validation
MPC for wind-power systems [2–5]	Partly considered	Not the main focus	Usually not attack-aware	No	No	Limited
Robust/stochastic control and estimation [9–13]	Considered	Not the main focus	Considered	Usually no	No	Problem-dependent
FDI detection and cyber-attack studies [15,16,18–20]	Partly considered	Considered	Partly considered	Considered	Usually not linked to MPC stability	Limited
Secure/resilient control under attacks [6,7,21–24]	Partly considered	Considered	Partly considered	Partly considered	Rarely incorporated as bounded perturbation	Limited
Proposed EKF- χ^2 -RLMPC	Considered	Bounded stochastic FDI	Attack-aware EKF	Considered	Included in bounded stability analysis	Monte Carlo and ablation baselines

Motivated by these observations, this paper addresses the secure high-performance control problem of wind power systems under stochastic disturbances and bounded stochastic FDI attacks. An EKF-RLMPC method is developed to link residual-based attack de-

tection, state estimation and Lyapunov-based predictive optimization within a unified framework. The main contributions are summarized as follows:

1. An EKF-based state estimation scheme is introduced to improve state reconstruction for wind power systems under process and measurement noise. A residual-based chi-square (χ^2) detector is designed for EKF estimator to detect the FDI attacks.
2. The state estimate and detection results are incorporated into the RLMPC framework to construct an EKF-RLMPC control strategy for incomplete information. At each sampling instant, the RLMPC optimization is solved using the current reliable EKF estimate, and the first element of the optimal input sequence is applied to the wind power systems.
3. Closed-loop stability is established and simulation studies demonstrate the effectiveness of the proposed method in improving state estimation accuracy, enhancing robustness, and mitigating the adverse effects of FDI attacks.

2. Problem Formulation

The nonlinear wind power model adopted from [2] is used as the nominal plant, and stochastic disturbances and FDI attacks are introduced in this work. The state equation can be represented as

$$\dot{x}(t) = f(x(t), u(t), v(t)) = \begin{bmatrix} \frac{1}{J_g N_g} \left(-N_g u_2(t) - \frac{B_\theta}{N_g} x_1(t) + B_\theta x_2(t) + K_\theta x_3(t) \right) \\ \frac{1}{J_a} \left(T_a(t) + \frac{B_\theta}{N_g} x_1(t) - B_\theta x_2(t) - K_\theta x_3(t) \right) \\ x_2(t) - \frac{1}{N_g} x_1(t) \end{bmatrix} \quad (1)$$

with the measured state output

$$y(t) = Cx(t) \quad (2)$$

where $x(t) = [\omega_g(t) \ \omega_a(t) \ \theta(t)]^T$ collects the generator-side speed, turbine-side speed, and shaft torsional angle; $u(t) = [\beta(t) \ T_g(t)]^T$ contains the pitch angle and generator torque, with $u_2(t) = T_g(t)$. The generator output matrix is $C = I_3$. The parameters J_g and J_a are the generator and turbine inertias, N_g is the gearbox ratio, B_θ and K_θ describe drivetrain damping and stiffness, T_a is the aerodynamic torque, v is the wind speed, and η denotes the generator conversion efficiency.

From a control-oriented positive-real (PR) and passivity-related perspective, the wind power plant can be interpreted as an energy-exchange system. The inertias J_g and J_a characterize kinetic-energy storage in the generator and turbine rotors, K_θ characterizes the elastic energy stored in the flexible shaft, B_θ represents drivetrain dissipation, and N_g determines the speed–torque transformation between the turbine and generator sides. The input quantities $\beta(t)$ and $T_g(t)$ affect aerodynamic energy capture and electromechanical torque extraction, whereas $P_g(t)$ is constrained as the regulated output-power quantity. These physical quantities are consistent with PR/passivity interpretations in which stored and dissipated energy determine the input–output behavior of a control plant. Recent results on the connection between bounded-real and positive-real characteristic values through scattering relations provide useful theoretical background for such interpretations [25]. Since the model considered is nonlinear, constrained, stochastic disturbances, FDI attacks and model mismatch, this paper does not rely on a strict linear transfer-function PR representation. Instead, the above physical energy features motivate the Lyapunov-type function and compact admissible sets used in the RLMPC stability analysis.

Since $y(t)$ is selected as the measured state vector, the considered FDI attack acts on the state measurements delivered to the estimator rather than directly on the physical plant. Consider the wind power system subject to stochastic disturbances during operation. By incorporating process disturbances and measurement noise, the compact state-space representation can be written as

$$\begin{aligned}\dot{x}(t) &= f(x(t), u(t), v(t)) + w(t) \\ y^a(t) &= Cx(t) + n(t)\end{aligned}\quad (3)$$

where y^a denotes the measured output, and w and n denote the process noise and measurement noise, respectively. Considering wind-speed fluctuations, aerodynamic uncertainty, sensor-accuracy limitations, and other factors in wind power systems, the noise terms are assumed to satisfy the following boundedness constraints:

$$w \in \mathbb{W} := \{w \in \mathbb{R}^3 : |w| \leq \bar{w}\} \quad (4)$$

$$n \in \mathbb{N} := \{n \in \mathbb{R}^3 : |n| \leq \bar{n}\} \quad (5)$$

where $\mathbb{W}$ and $\mathbb{N}$ denote the admissible sets of the process and measurement noise, respectively, and $\bar{w}, \bar{n} > 0$ are known constants.

In addition, the control input, system state, and output power are constrained by physical and actuator limitations and satisfy:

$$u \in \mathbb{U}, x \in \mathbb{X}, P_g \in \mathbb{P} \quad (6)$$

To mitigate the influence of stochastic disturbances on measured system states, a state estimator is required to filter the measurement signals. In practical implementation, state estimation is usually performed through prediction and correction steps based on the nonlinear discrete-time model. By discretizing the continuous-time wind power system at the sampling instants, the following form is obtained:

$$\begin{aligned}x(t_{k+1}) &= F(x(t_k), u(t_k), v(t_k), w(t_k)) \\ y^a(t_k) &= Cx(t_k) + n(t_k)\end{aligned}\quad (7)$$

where $F(x(t_k), u(t_k), v(t_k), w(t_k))$ denotes the discrete-time mapping generated by the nonlinear system evolution over the sampling interval $[t_k, t_{k+1}]$, namely the integration of the continuous-time model over this interval.

On the basis of the wind power system model (3) with process and measurement noise, FDI attacks are further introduced to study the control problem. Specifically, an FDI attack model is constructed for the sensor-to-estimator (S-E) communication channel.

In this model, the state measurements may be compromised by FDI attacks during transmission, which distorts the measurement information received by the estimator. Under the combined effects of FDI attacks, stochastic disturbances, measurement noise, and bounded model mismatch, the state-space model becomes:

$$\begin{aligned}\dot{x}(t) &= f(x(t), u(t), v(t)) + w(t) + \Delta_f(t), \\ y^a(t_k) &= Cx(t_k) + n(t_k) + \vartheta(t_k)a(t_k),\end{aligned}\quad (8)$$

where $y^a(t_k)$ denotes the measurement received by the estimator, $n(t_k)$ is the measurement noise, $a(t_k)$ is the injected FDI signal, and $\vartheta(t_k) \in \{0, 1\}$ is the attack occurrence indicator. The term $\Delta_f(t)$ represents bounded model mismatch caused by parameter variations, unmodeled nonlinearities, and aerodynamic uncertainty in wind power systems.

The attack signal and model mismatch are assumed to be bounded:

$$\|a(t_k)\| \leq \bar{a}, \quad \|\Delta_f(t)\| \leq \bar{\Delta}_f, \quad (9)$$

where $\bar{a} > 0$ and $\bar{\Delta}_f > 0$ are known constants. For the proportional FDI case considered in the simulations, the injected signal can be expressed as

$$a(t_k) = \Delta(t_k)Cx(t_k), \quad \|\Delta(t_k)\| \leq \bar{\Delta}, \quad (10)$$

where $\Delta(t_k)$ is a bounded random matrix.

Furthermore, $\vartheta(t_k)$ is modeled as a Bernoulli random variable satisfying:

$$\mathbb{E}\{\vartheta(t_k)\} = \Pr\{\vartheta(t_k) = 1\} = \bar{\vartheta} \quad (11)$$

where $0 \leq \bar{\vartheta} \leq 1$ denotes the occurrence probability of FDI attacks.

When $\vartheta(t_k) = 1$, the system is subject to an FDI attack and the transmitted measurement data are maliciously tampered with. When $\vartheta(t_k) = 0$, communication is normal and the estimator receives the uncorrupted measurement information. To reflect realistic constraints on attack behavior, the duration of consecutive attacks is assumed to be upper bounded. Specifically, there exists a positive integer N_a such that the number of consecutive FDI attack steps does not exceed this bound, thereby excluding the extreme case of indefinitely persistent attacks. That is, this work focuses on bounded stochastic FDI attacks injected into the sensor-to-estimator channel. This setting describes random and intermittent measurement falsification attacks with bounded attack magnitude.

Considering FDI attacks on the S-E channel, this section develops an EKF-RLMPC control framework for wind power systems, as shown in Figure 1. First, measurement data may be corrupted by FDI attacks during transmission, leading to distorted information at the estimator input. Second, an attack detection mechanism is embedded in the estimator to assess measurement credibility. Specifically, the estimator adaptively adjusts the EKF update according to the detection result: when the measurement is credible, the standard correction step is performed; otherwise, the measurement correction is suppressed. The RLMPC controller then uses the resulting EKF estimate at every sampling instant to solve the finite-horizon optimization problem and update the applied control input to prevent abnormal measurements.

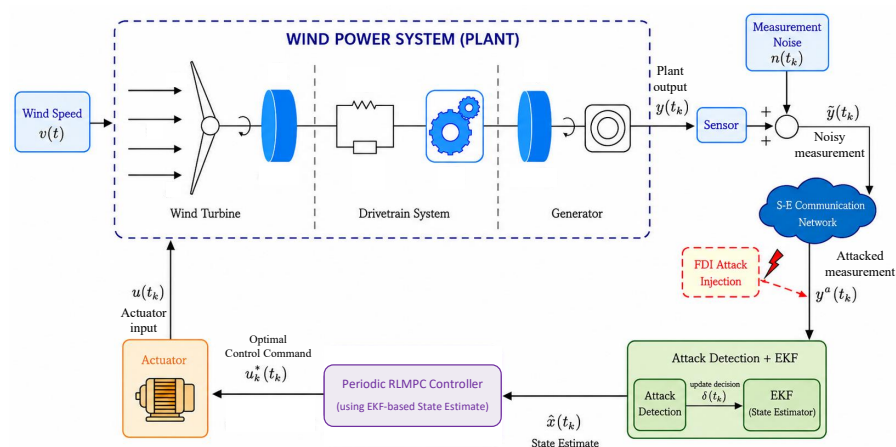


Figure 1. EKF-RLMPC control diagram for wind power systems under FDI attacks.

3. EKF-RLMPC Control for Wind Power Systems Under FDI Attacks

3.1. Design of the Resilient State Estimator

Since FDI attacks may distort or interrupt measurement data and reduce the reliability of state estimation, this section designs a resilient state estimator. Specifically, a residual-based chi-square (χ^2) detection mechanism is incorporated into the EKF framework to identify abnormal measurements and enhance estimator robustness and security. At time t_k , the residual between the received measurement and the EKF prior estimate is defined as:

$$\epsilon_r(t_k) = y^a(t_k) - C\hat{x}^-(t_k) \quad (12)$$

The covariance matrix of the residual is given by:

$$S(t_k) = CP^-(t_k)C^T + R \quad (13)$$

where $P^-(t_k)$ is the prior covariance matrix and $R \in \mathbb{R}^{3 \times 3}$ is the measurement-noise covariance matrix.

Based on the above residual, the following χ^2 statistic is constructed:

$$J(t_k) = \epsilon_r^T(t_k)S^{-1}(t_k)\epsilon_r(t_k) \quad (14)$$

In the ideal case without attacks and with only Gaussian noise, the statistic $J(t_k)$ follows a χ^2 distribution with degrees of freedom equal to the measurement dimension $n_y = 3$, namely:

$$J(t_k) \sim \chi^2(n_y) \quad (15)$$

For a given significance level $\gamma \in (0, 1)$, the detection threshold μ_a is selected such that:

$$\Pr\{J(t_k) \leq \mu_a\} = 1 - \gamma \quad (16)$$

Based on the χ^2 statistic, the following attack decision rule is constructed:

$$\delta(t_k) = \begin{cases} 1, & J(t_k) > \mu_a \\ 0, & J(t_k) \leq \mu_a \end{cases} \quad (17)$$

where $\delta(t_k) = 1$ indicates that an FDI attack is detected, and $\delta(t_k) = 0$ indicates that the measurement data are credible.

Since the residual-based detector is affected by process disturbances, measurement noise, model mismatch, and attack amplitude, the detected attack indicator $\delta(t_k)$ may be different from the true attack occurrence indicator $\vartheta(t_k)$. The case $\delta(t_k) = 1, \vartheta(t_k) = 0$ corresponds to a false alarm, whereas $\delta(t_k) = 0, \vartheta(t_k) = 1$ corresponds to a missed detection.

Using the detection result, the EKF correction step is modified as follows:

- When $\delta(t_k) = 1$:

$$K(t_k) = 0, \hat{x}(t_k) = \hat{x}^-(t_k), P(t_k) = P^-(t_k) \quad (18)$$

- When $\delta(t_k) = 0$:

$$K(t_k) = P^-(t_k)C^T[CP^-(t_k)C^T + R]^{-1} \quad (19)$$

$$\hat{x}(t_k) = \hat{x}^-(t_k) + K(t_k)\epsilon_r(t_k) \quad (20)$$

$$P(t_k) = (I - K(t_k)C)P^-(t_k) \quad (21)$$

By introducing the residual-based χ^2 detection mechanism, the resilient state estimator can identify abnormal measurements under FDI attacks. When an attack is detected, the estimator relies on model prediction instead of corrupted measurements, preserving the continuity of the estimation process. The estimator improves state-estimation reliability with limited additional computational complexity and provides credible state information for the subsequent resilient control design.

3.2. Design of Resilient LMPC with FDI Attack Detection and EKF

Since FDI attacks may corrupt measurement information and reduce the reliability of the estimated state, this section adopts a periodic receding-horizon optimization mechanism. Under this mechanism, the controller does not evaluate a conditional update rule; instead, the RLMPC optimization problem is solved at every sampling instant. The objective is to ensure periodic controller updating while the EKF measurement update remains protected by the residual-based χ^2 attack detector. The periodic receding-horizon optimization mechanism is given as follows:

- (1) At each sampling instant $t_k = t_0 + k\Delta$, the controller receives the current posterior EKF estimate $\hat{x}(t_k)$. This estimate is obtained either by the standard measurement-correction step when the measurement is credible or by the model-prediction step when an FDI attack is detected. Therefore, the input to the RLMPC optimization is always the attack-detection-based state estimate rather than the raw measurement.
- (2) The RLMPC optimization computation is performed periodically at every sampling instant. No auxiliary update variable, inter-update interval, state-error threshold, or filter-based conditional criterion is introduced. Accordingly, the controller directly solves the current optimization problem using the latest posterior EKF estimate.
- (3) When an FDI attack is detected, the measurement correction in the EKF is suppressed, but the RLMPC optimization is still solved using the model-predicted posterior estimate $\hat{x}(t_k) = \hat{x}^-(t_k)$. Thus, the controller is not frozen under attacks; instead, it continues to compute the control input from the best available reliable state estimate provided by the resilient estimator.

Over the operating interval $[t_0, t_f]$, the RLMPC optimization problem is solved at each sampling instant using the posterior EKF estimate. Based on the preceding periodic receding-horizon mechanism, the EKF-RLMPC algorithm is invoked at every sampling instant t_k to compute the control input. Specifically, for system (3), the optimization problem is formulated as:

$$\min_{u_k \in S(\Delta)} \int_{t_k}^{t_{k+N}} \|\Delta \tilde{z}(\tau)\|_q^2 d\tau + \sum_{n=k+1}^{k+N-1} \|\Delta u(t_n)\|_p^2 \quad (22)$$

subject to:

$$\dot{\tilde{x}}(t) = f(\tilde{x}(t), u_k(t), \tilde{v}(t)), \forall t \in [t_k, t_{k+N}) \quad (23a)$$

$$\tilde{y}(t) = C\tilde{x}(t), \forall t \in [t_k, t_{k+N}) \quad (23b)$$

$$\tilde{x}(t_k) = \tilde{x}(t_k) = \hat{x}(t_k) \quad (23c)$$

$$\dot{\tilde{x}}(t) = f(\tilde{x}(t), h(\tilde{x}(t_j)), \tilde{v}(t)), \forall t \in [t_j, t_{j+1}) \quad (23d)$$

$$V(\tilde{x}(t)) \leq V(\tilde{x}(t)), \forall t \in [t_k, t_{k+N}) \quad (23e)$$

$$\tilde{x}, \tilde{x} \in \mathbb{X}, u_k \in \mathbb{U}, \tilde{P}_g \in \mathbb{P} \quad (23f)$$

In this optimization problem, $\hat{x}$ denotes the posterior state estimate provided by the resilient EKF. The term $\|\Delta \tilde{z}(\tau)\|_q^2$ penalizes the deviation of the predicted output or state-related performance variable from the desired operating region of the wind power system, while $\|\Delta u(t_n)\|_p^2$ penalizes excessive control variations and avoids aggressive actuator actions.

The Lyapunov constraint in (23e) is introduced to enforce a stability-oriented decrease condition along the nominal prediction trajectory. During prediction, stochastic noise, FDI-induced perturbations, detection errors, and model mismatch are not directly propagated in the nominal model; instead, their influence is handled through the EKF estimation-error bound and the robust Lyapunov-based stability analysis.

At each sampling instant, the optimization problem (22) is solved using the current posterior state estimate provided by the resilient EKF. The actual control input applied to the wind power system is generated from the RLMPC solution obtained at the same sampling instant:

$$u(t_k) = u_k^*(t_k). \quad (24)$$

Combining the resilient state estimator with the periodic RLMPC optimization mechanism, the implementation procedure of the EKF-RLMPC algorithm is summarized in Algorithm 1.

Algorithm 1 EKF-RLMPC algorithm for wind power systems under FDI attacks

```

1: Set the total number of sampling instants  $t_f$ , prediction horizon  $N$ , maximum number of consecutive attacks  $N_a$ , attack probability  $\bar{\theta}$ , attack detection threshold  $\mu_a$ , state weight  $q$ , input weight  $p$ , process-noise parameter  $\theta_w$ , and measurement-noise parameter  $\theta_n$ ;
2: Initialization:  $k = 0, \hat{x}(t_0), P(t_0)$ ;
3: Perform the initial optimization at time  $t_0$  to obtain the initial control input sequence;
4: while  $t_k \in [t_0, t_f]$  do
5:   // Sensor
6:   Generate the FDI attack variable  $\vartheta(t_k)$  and attack signal  $a(t_k)$ ;
7:    $y^a(t_k) = Cx(t_k) + n(t_k) + \vartheta(t_k)a(t_k)$ ;
8:   //  $\chi^2$  attack detection
9:    $\hat{x}^-(t_k) = F(\hat{x}(t_{k-1}), u(t_{k-1}), v(t_{k-1}), 0)$ ;
10:   $P^-(t_k) = A(t_{k-1})P(t_{k-1})A^T(t_{k-1}) + Q$ ;
11:   $e_r(t_k) = y^a(t_k) - C\hat{x}^-(t_k)$ ;
12:   $S(t_k) = CP^-(t_k)C^T + R$ ;
13:   $J(t_k) = e_r^T(t_k)S^{-1}(t_k)e_r(t_k)$ ;
14:  if  $J(t_k) > \mu_a$  then
15:    Identify an FDI attack:  $\delta(t_k) = 1$ ;
16:  else
17:    Identify normal operation:  $\delta(t_k) = 0$ ;
18:  end if
19:  // EKF based on attack detection
20:  if  $\delta(t_k) = 1$  then
21:     $K(t_k) = 0$ ;
22:  else
23:     $K(t_k) = P^-(t_k)C^T[CP^-(t_k)C^T + R]^{-1}$ ;
24:  end if
25:   $\hat{x}(t_k) = \hat{x}^-(t_k) + K(t_k)[y^a(t_k) - C\hat{x}^-(t_k)]$ ;
26:   $P(t_k) = (I - K(t_k)C)P^-(t_k)$ ;
27:  // Controller (periodic RLMPC)
28:  Solve the RLMPC optimization problem using the current posterior EKF estimate and obtain  $u_k^* = \{u_k^*(t_k), \dots, u_k^*(t_{k+N-1})\}$ ;
29:  Apply the first element of the current optimal input sequence:  $u_a(t_k) = u_k^*(t_k)$ ;
30:  // Actuator
31:   $u(t_k) = u_a(t_k)$ ;
32:  // System update
33:   $f(x(t_k), u(t_k), v(t_k)) + w(t_k) + \Delta_f(t_k) \Rightarrow x(t_{k+1})$ ;
34:   $k = k + 1$ ;
35: end while

```

3.3. Stability Analysis

3.3.1. Boundedness of the EKF Estimation Error

To analyze the influence of FDI attacks on state-estimation performance, attack-induced terms, detection errors, and bounded model mismatch are introduced into the EKF framework, and the corresponding error dynamics are reconstructed.

Under the attacked measurement model (8), the innovation used by the EKF can be written as

$$\epsilon_r(t_k) = y^a(t_k) - C\hat{x}^-(t_k). \quad (25)$$

Substituting $y^a(t_k) = Cx(t_k) + n(t_k) + \vartheta(t_k)a(t_k)$ into (25) yields

$$\epsilon_r(t_k) = C(x(t_k) - \hat{x}^-(t_k)) + n(t_k) + \vartheta(t_k)a(t_k). \quad (26)$$

Therefore, the FDI signal directly enters the EKF innovation term. Since the residual-based detector is also affected by process disturbances, measurement noise, model mismatch, and attack amplitude, the detected attack indicator $\delta(t_k)$ may be different from the true attack occurrence indicator $\vartheta(t_k)$. The case $\delta(t_k) = 1, \vartheta(t_k) = 0$ corresponds to a false alarm, whereas $\delta(t_k) = 0, \vartheta(t_k) = 1$ corresponds to a missed detection. Their influence is treated as an equivalent bounded perturbation in the following analysis.

Assumption 1. Assume that the wind power generation system is locally observable, that is, the local observability matrix constructed from the linearized pair $(A(t_k), C)$ is full rank at any time instant $k \geq 0$. In addition, the system Jacobian matrix $A(t_k)$ is full rank at each time instant.

Assumption 2. The equivalent perturbation induced by FDI attacks, detection errors, and model mismatch is bounded. Specifically, define the lumped perturbation as

$$d_c(t_k) = d_a(t_k) + d_\delta(t_k) + d_f(t_k), \quad (27)$$

where $d_a(t_k)$ denotes the perturbation caused by the injected FDI signal, $d_\delta(t_k)$ denotes the perturbation caused by false alarms or missed detections of the residual-based detector, and $d_f(t_k)$ denotes the perturbation caused by bounded model mismatch. There exists a constant $\bar{D}_c > 0$ such that

$$\|d_c(t_k)\| \leq \bar{D}_c. \quad (28)$$

Lemma 1. Under Assumptions 1 and 2, the prior error dynamics can be uniformly expressed as [14]:

$$e^-(t_{k+1}) = A(t_k)e(t_k) + r(t_k), \quad (29)$$

where

$$r(t_k) = \phi(\cdot) + G(t_k)w(t_k) + d_c(t_k). \quad (30)$$

Moreover, there exist $\bar{\epsilon}$, a constant $\lambda_\phi > 0$, and class- $\mathcal{K}$ functions ι_1, ι_2 such that, for $\|e\| \leq \bar{\epsilon}$,

$$\|r(t_k)\| \leq \lambda_\phi \|e(t_k)\|^2 + \iota_1(\|w(t_k)\|) + \iota_2(\|d_c(t_k)\|). \quad (31)$$

Theorem 1. Under Assumptions 1 and 2, consider the attack-detection-based EKF with the following update strategy:

$$K(t_k) = \begin{cases} 0, & \delta(t_k) = 1, \\ P^-(t_k)C^T[CP^-(t_k)C^T + R]^{-1}, & \text{otherwise.} \end{cases}$$

The detector is not required to be perfect. The influence of false alarms, missed detections, and model mismatch is included in the bounded lumped perturbation $d_c(t_k)$. Then there exist positive constants $\alpha_0 > 0$, $\beta_0 > 1$, and class- $\mathcal{K}$ functions $\iota_w(\cdot)$, $\iota_d(\cdot)$ such that the posterior estimation error is bounded as follows:

$$|e(t_k)| \leq \alpha_0 \|e(t_0)\| \beta_0^{-k} + \iota_w \left(\sup_{0 \leq i \leq k} \|w(t_i)\| \right) + \iota_d \left(\sup_{0 \leq i \leq k} \|d_c(t_i)\| \right). \quad (32)$$

Proof. From the prior error dynamics, it follows that:

$$e(t_{k+1}) = (I - K(t_k)C)(A(t_k)e(t_k) + r(t_k)). \quad (33)$$

Let $M_k = (I - K(t_k)C)A(t_k)$. Then:

$$e(t_{k+1}) = M_k e(t_k) + (I - K(t_k)C)r(t_k). \quad (34)$$

Construct the Lyapunov function:

$$V(e(t_k)) = e^T(t_k)\Pi(t_k)e(t_k). \quad (35)$$

Combining the above relations yields:

$$\begin{aligned} V(e(t_{k+1})) &= e^T(t_k)M_k^T\Pi(t_{k+1})M_k e(t_k) \\ &\quad + 2e^T(t_k)M_k^T\Pi(t_{k+1})(I - KC)r(t_k) \\ &\quad + r^T(t_k)(I - KC)^T\Pi(t_{k+1})(I - KC)r(t_k). \end{aligned} \quad (36)$$

Applying Young's inequality to bound the cross term and using matrix boundedness gives:

$$V(e(t_{k+1})) \leq \rho V(e(t_k)) + \sigma \|r(t_k)\|^2, \quad (37)$$

where $\rho \in (0, 1)$ and $\sigma > 0$ are constants.

By Lemma 1,

$$\|r(t_k)\| \leq \lambda_\phi \|e(t_k)\|^2 + \iota_1(\|w(t_k)\|) + \iota_2(\|d_c(t_k)\|). \quad (38)$$

Squaring both sides of the preceding inequality and using $(a + b + c)^2 \leq 3(a^2 + b^2 + c^2)$ gives:

$$\|r(t_k)\|^2 \leq 3\lambda_\phi^2 \|e(t_k)\|^4 + 3\iota_1^2(\|w(t_k)\|) + 3\iota_2^2(\|d_c(t_k)\|). \quad (39)$$

On the bounded error set $\|e(t_k)\| \leq \bar{\epsilon}$,

$$\|e(t_k)\|^4 \leq \bar{\epsilon}^2 \|e(t_k)\|^2. \quad (40)$$

By the definition of the Lyapunov function, there exists a constant $c_1 > 0$ such that:

$$\|e(t_k)\|^2 \leq \frac{1}{c_1} V(e(t_k)). \quad (41)$$

Substituting (41) into (39) and multiplying both sides by σ gives:

$$\sigma \|r(t_k)\|^2 \leq cV(e(t_k)) + \tilde{\iota}_1(\|w(t_k)\|) + \tilde{\iota}_2(\|d_c(t_k)\|), \quad (42)$$

where $c = \frac{3\sigma\lambda_\phi^2\bar{\epsilon}^2}{c_1}$ is a constant, and $\tilde{\iota}_1, \tilde{\iota}_2$ are class- $\mathcal{K}$ functions.

Substituting (42) into (37) gives:

$$V(e(t_{k+1})) \leq \rho_c V(e(t_k)) + \tilde{\iota}_1(\|w(t_k)\|) + \tilde{\iota}_2(\|d_c(t_k)\|), \quad (43)$$

where $\rho_c = \rho + c \in (0, 1)$. This local contraction can be ensured by selecting the local error set sufficiently small, which is consistent with the EKF local boundedness condition.

Recursively expanding the above inequality with respect to k gives:

$$V(e(t_k)) \leq \rho_c^k V(e(t_0)) + \sum_{i=0}^{k-1} \rho_c^{k-1-i} [\tilde{\iota}_1(\|w(t_i)\|) + \tilde{\iota}_2(\|d_c(t_i)\|)]. \quad (44)$$

Since $0 < \rho_c < 1$, the boundedness of the geometric series implies that

$$\sum_{i=0}^{k-1} \rho_c^{k-1-i} \leq \frac{1}{1 - \rho_c}. \quad (45)$$

Therefore,

$$V(e(t_k)) \leq \rho_c^k V(e(t_0)) + \frac{1}{1 - \rho_c} \left[\sup_{0 \leq i \leq k} \tilde{\iota}_1(\|w(t_i)\|) + \sup_{0 \leq i \leq k} \tilde{\iota}_2(\|d_c(t_i)\|) \right]. \quad (46)$$

By the equivalence property of the Lyapunov function, there exists a constant $c_2 > 0$ such that:

$$V(e(t_0)) \leq c_2 \|e(t_0)\|^2. \quad (47)$$

Combining (41), (46), and (47) yields:

$$\|e(t_k)\|^2 \leq \frac{c_2}{c_1} \rho_c^k \|e(t_0)\|^2 + \frac{1}{c_1(1 - \rho_c)} \left[\sup_{0 \leq i \leq k} \tilde{\iota}_1(\|w(t_i)\|) + \sup_{0 \leq i \leq k} \tilde{\iota}_2(\|d_c(t_i)\|) \right]. \quad (48)$$

Taking the square root on both sides and using the closure property of class- $\mathcal{K}$ functions, one obtains:

$$\|e(t_k)\| \leq \alpha_0 \|e(t_0)\| \beta_0^{-k} + \iota_w \left(\sup_{0 \leq i \leq k} \|w(t_i)\| \right) + \iota_d \left(\sup_{0 \leq i \leq k} \|d_c(t_i)\| \right). \quad (49)$$

Since $d_c(t_k)$ is bounded by Assumption 2, the posterior estimation error remains bounded even when false alarms or missed detections occur, provided that their induced perturbations are bounded. This completes the proof. $\square$

According to Theorem 1, the posterior estimation error of the attack-detection-based EKF is bounded, i.e., $\|e(t_k)\| \leq e_k$, where

$$e_k = \alpha_0 \|e(t_0)\| \beta_0^{-k} + \iota_w \left(\sup_{0 \leq i \leq k} \|w(t_i)\| \right) + \iota_d \left(\sup_{0 \leq i \leq k} \|d_c(t_i)\| \right). \quad (50)$$

3.3.2. Closed-Loop Stability Under RLMPC

To complete the closed-loop analysis of the periodic EKF-RLMPC scheme, the following results are given by connecting the bounded EKF estimation error with the Lyapunov constraint used in the RLMPC optimization problem.

Lemma 2. *There exists a continuously differentiable Lyapunov function $V(x)$ and a locally stabilizing feedback law $u = h(x) \in \mathbb{U}$ such that, for all x in the compact set $\Omega_\rho := \{x \in \mathbb{X} : V(x) \leq \rho\}$ and all admissible wind speeds $v \in \mathbb{V}$, the following relations hold [26,27]:*

$$\beta_1(\|x\|) \leq V(x) \leq \beta_2(\|x\|), \quad (51)$$

$$\left\| \frac{\partial V(x)}{\partial x} \right\| \leq \beta_4(\|x\|), \quad (52)$$

$$\frac{\partial V(x)}{\partial x} f(x, h(x), v) \leq -\beta_3(\|x\|), \quad (53)$$

where $\beta_i(\cdot)$, $i = 1, 2, 3, 4$, are class- $\mathcal{K}$ functions. Moreover, there exist positive constants M , L_x , and L_v such that, for all $x, x' \in \Omega_\rho$, $u \in \mathbb{U}$, and $v, v' \in \mathbb{V}$,

$$\|f(x, u, v)\| \leq M, \quad (54)$$

$$\|f(x, u, v) - f(x', u, v')\| \leq L_x \|x - x'\| + L_v \|v - v'\|. \quad (55)$$

The wind-speed prediction error is bounded as $\|v(t) - \tilde{v}(t)\| \leq \bar{\delta}_v$, and the RLMPC optimization problem remains feasible for all sampling instants considered.

Lemma 3. Under the conditions of Lemma 2, for any $x, x' \in \Omega_\rho$, there exists a nonnegative increasing function $f_V(\cdot)$ such that [26]

$$V(x) \leq V(x') + f_V(\|x - x'\|). \quad (56)$$

In particular, $f_V(\tau)$ can be chosen in the quadratic form

$$f_V(\tau) = \beta_4 \left(\beta_1^{-1}(\rho) \right) \tau + \alpha \tau^2, \quad (57)$$

where $\alpha > 0$ is a constant.

Lemma 4. Consider the auxiliary trajectory $\check{x}(t)$ generated by the stabilizing feedback law $u = h(\check{x}(t_j))$ over the sampling interval $[t_j, t_{j+1})$, namely [27],

$$\dot{\check{x}}(t) = f(\check{x}(t), h(\check{x}(t_j)), \tilde{v}(t)), \quad t \in [t_j, t_{j+1}). \quad (58)$$

Under the conditions of Lemma 2, there exist constants $\Delta > 0$, $\varepsilon_s > 0$, and $\rho > \rho_s > \rho_{\min} > 0$ such that, for $\check{x}(t_j) \in \Omega_\rho$,

$$V(\check{x}(t)) \leq V(\check{x}(t_j)), \quad \forall t \in [t_j, t_{j+1}), \quad (59)$$

$$V(\check{x}(t_{j+1})) \leq \max\{V(\check{x}(t_j)) - \varepsilon_s, \rho_{\min}\}. \quad (60)$$

The model-mismatch component $d_f(t_k)$ in Assumption 2 characterizes its influence on the EKF estimation-error dynamics, whereas Lemma 5 further accounts for the mismatch between the actual closed-loop trajectory and the nominal RLMPC prediction trajectory. Thus, the two appearances of model mismatch correspond to the estimator-side error analysis and the controller-side prediction-error analysis, respectively.

Lemma 5. Consider the actual closed-loop trajectory and the nominal prediction trajectory of the wind power system over the sampling interval $[t_k, t_k + \tau]$, where $0 \leq \tau \leq \Delta$. Let $x_a(t)$ denote the actual system state and $\tilde{x}(t)$ denote the nominal state predicted by the RLMPC model. Suppose that the actual and nominal trajectories satisfy [27]

$$\begin{aligned} \dot{x}_a(t) &= f(x_a(t), u(t), v(t)) + w(t) + \Delta_f(t), \\ \dot{\tilde{x}}(t) &= f(\tilde{x}(t), u(t), \tilde{v}(t)), \end{aligned} \quad (61)$$

where $u(t) \in \mathbb{U}$ is the applied control input, $v(t)$ and $\tilde{v}(t)$ are the actual and predicted wind speeds, respectively, $w(t)$ is the process disturbance, and $\Delta_f(t)$ is the bounded model mismatch. Assume that $x_a(t), \tilde{x}(t) \in \Omega_p$, $u(t) \in \mathbb{U}$, $\|v(t) - \tilde{v}(t)\| \leq \bar{\delta}_v$, $\|w(t)\| \leq \bar{w}$, and $\|\Delta_f(t)\| \leq \bar{\Delta}_f$. Then, by Lemma 2, there exists a bounded function $\chi_k(\tau)$ such that

$$\|x_a(t_k + \tau) - \tilde{x}(t_k + \tau)\| \leq \chi_k(\tau), \quad (62)$$

where

$$\chi_k(\tau) = e^{L_x \tau} e_k + \frac{e^{L_x \tau} - 1}{L_x} (L_v \bar{\delta}_v + \bar{w} + \bar{\Delta}_f), \quad (63)$$

and e_k is the posterior EKF estimation-error bound obtained in Theorem 1.

Proof. Let the mismatch between the actual trajectory and the nominal RLMPc prediction be

$$e_p(t) = x_a(t) - \tilde{x}(t). \quad (64)$$

Subtracting the nominal prediction model from the disturbed plant dynamics gives

$$\dot{e}_p(t) = f(x_a(t), u(t), v(t)) - f(\tilde{x}(t), u(t), \tilde{v}(t)) + w(t) + \Delta_f(t). \quad (65)$$

The Lipschitz bound in Lemma 2 then yields the following estimate for the error dynamics

$$\|\dot{e}_p(t)\| \leq L_x \|x_a(t) - \tilde{x}(t)\| + L_v \|v(t) - \tilde{v}(t)\| + \|w(t)\| + \|\Delta_f(t)\|. \quad (66)$$

Using the bounds on the wind-speed prediction error, process disturbance, and model mismatch, this estimate reduces to

$$\|\dot{e}_p(t)\| \leq L_x \|e_p(t)\| + L_v \bar{\delta}_v + \bar{w} + \bar{\Delta}_f. \quad (67)$$

At t_k , the nominal trajectory starts from the EKF posterior estimate, i.e., $\tilde{x}(t_k) = \hat{x}(t_k)$. Therefore,

$$\|e_p(t_k)\| = \|x_a(t_k) - \hat{x}(t_k)\| \leq e_k. \quad (68)$$

The comparison lemma applied on $[t_k, t_k + \tau]$ gives

$$\|e_p(t_k + \tau)\| \leq e^{L_x \tau} \|e_p(t_k)\| + \int_{t_k}^{t_k + \tau} e^{L_x(t_k + \tau - s)} (L_v \bar{\delta}_v + \bar{w} + \bar{\Delta}_f) ds. \quad (69)$$

After evaluating the integral, the bound becomes

$$\|e_p(t_k + \tau)\| \leq e^{L_x \tau} e_k + \frac{e^{L_x \tau} - 1}{L_x} (L_v \bar{\delta}_v + \bar{w} + \bar{\Delta}_f). \quad (70)$$

Thus, the prediction mismatch satisfies (62) with $\chi_k(\tau)$ defined in (63). This completes the proof. $\square$

Theorem 2. Consider the wind power system under the attack-detection-based EKF and the periodic RLMPc controller. Suppose that Assumptions 1 and 2 hold, Lemma 2 applies, the RLMPc optimization problem (22)–(23) is feasible at each sampling instant, and the Lyapunov constraint in (23e) is imposed over the prediction horizon. The lumped perturbation $d_c(t_k)$, process disturbance $w(t_k)$, wind-speed prediction error, and model mismatch are assumed to be bounded. Let

$$\Delta, \varepsilon_s > 0, \quad \rho > \rho_s > \rho_{\min} > 0. \quad (71)$$

If

$$f_V(\bar{e}) + f_V(\bar{\chi}) - \varepsilon_s < 0, \quad (72)$$

and if $\rho_a < \rho$, then, for any initial condition $x(t_0) \in \Omega_\rho$, the closed-loop state of the EKF-RLMPC system is ultimately bounded and satisfies

$$\limsup_{k \rightarrow \infty} V(x(t_k)) \leq \rho_a. \quad (73)$$

Consequently, the state trajectory ultimately enters the compact set $\Omega_{\rho_a} := \{x \in \mathbb{X} : V(x) \leq \rho_a\} \subseteq \Omega_\rho$.

Proof. At each sampling instant, the periodic EKF-RLMPC controller solves the optimization problem (22) and (23) using the posterior EKF estimate $\hat{x}(t_k)$. Theorem 1 and Assumption 2 imply that the posterior EKF estimation-error bound is uniformly bounded even in the presence of bounded FDI-induced perturbations, detection errors, and model mismatch, and hence $\bar{e} = \sup_{k \geq 0} e_k < \infty$. Since the wind-speed prediction error, process disturbance, and model mismatch are bounded by $\bar{\delta}_v$, $\bar{w}$, and $\bar{\Delta}_f$, respectively, the definition of $\chi_k(\Delta)$ further gives $\bar{\chi} = \sup_{k \geq 0} \chi_k(\Delta) < \infty$. By (23c), the nominal prediction and the auxiliary trajectory are initialized as

$$\tilde{x}(t_k) = \check{x}(t_k) = \hat{x}(t_k). \quad (74)$$

From Lemma 4, the auxiliary trajectory satisfies

$$V(\check{x}(t_{k+1})) \leq \max\{V(\check{x}(t_k)) - \varepsilon_s, \rho_{\min}\}. \quad (75)$$

The Lyapunov constraint (23e) imposed in the RLMPC optimization gives

$$V(\tilde{x}(t_{k+1})) \leq V(\check{x}(t_{k+1})). \quad (76)$$

Combining (75) and (76) yields

$$V(\tilde{x}(t_{k+1})) \leq \max\{V(\check{x}(t_k)) - \varepsilon_s, \rho_{\min}\}. \quad (77)$$

Using (74), $V(\check{x}(t_k)) = V(\hat{x}(t_k))$. Since the true state and the posterior estimate satisfy $\|x(t_k) - \hat{x}(t_k)\| \leq e_k$, Lemma 3 gives

$$V(\hat{x}(t_k)) \leq V(x(t_k)) + f_V(e_k). \quad (78)$$

Substituting (78) into (77) gives

$$V(\tilde{x}(t_{k+1})) \leq \max\{V(x(t_k)) + f_V(e_k) - \varepsilon_s, \rho_{\min}\}. \quad (79)$$

Next, Lemma 5 implies $\|x(t_{k+1}) - \tilde{x}(t_{k+1})\| \leq \chi_k(\Delta)$. Applying Lemma 3 once more yields

$$V(x(t_{k+1})) \leq V(\tilde{x}(t_{k+1})) + f_V(\chi_k(\Delta)). \quad (80)$$

Combining (79) and (80), and using $e_k \leq \bar{e}$ and $\chi_k(\Delta) \leq \bar{\chi}$, we obtain

$$V(x(t_{k+1})) \leq \max\{V(x(t_k)) + f_V(\bar{e}) - \varepsilon_s, \rho_{\min}\} + f_V(\bar{\chi}). \quad (81)$$

Equivalently,

$$V(x(t_{k+1})) \leq \max\{V(x(t_k)) - \varepsilon_c, \rho_a\}, \quad (82)$$

where

$$\varepsilon_c := \varepsilon_s - f_V(\bar{e}) - f_V(\bar{\chi}) > 0 \quad (83)$$

by condition (72), and ρ_a is defined in (71). Inequality (82) shows that whenever $V(x(t_k)) > \rho_a$, the Lyapunov value decreases by at least ε_c at the next sampling instant. Therefore, after a finite number of sampling instants, $V(x(t_k))$ enters the set $\{V(x) \leq \rho_a\}$ and remains bounded there. Recursively applying (82) gives

$$\limsup_{k \rightarrow \infty} V(x(t_k)) \leq \rho_a. \quad (84)$$

Thus, the closed-loop state of the EKF-RLMPC system is ultimately bounded in Ω_{ρ_a} . This completes the proof. $\square$

4. Simulation Validation

4.1. Environment Settings

To evaluate the proposed EKF-RLMPC control strategy for wind power systems under FDI attacks, this section presents simulation studies based on the preceding theoretical analysis. To isolate the influence of attacks on system performance, the process and measurement noise levels are fixed at $\theta_w = 0.01$ and $\theta_n = 0.01$, respectively, thereby avoiding additional effects caused by noise-parameter variations. The main simulation parameters used in the revised Monte Carlo validation are summarized in Table 2.

The residual threshold $\mu_a = 80$ is selected as a conservative detection threshold for the considered nonlinear wind-power simulation with stochastic disturbances and bounded model mismatch. This setting avoids excessive false alarms, while the possible missed detections are reported through the Monte Carlo statistics and are also covered by the bounded-perturbation stability analysis.

Table 2. Main simulation parameters used in the EKF-RLMPC validation.

Parameter	Value	Description
T_s	0.05 s	Sampling interval
h	0.01 s	Numerical integration step
N	6	Prediction horizon of RLMPC
q_{low}	$[1.0 \times 10^{-3}, 6.0 \times 10^7]$	State/output weights under low wind speed
p_{low}	$[1.0 \times 10^7, 5.0 \times 10^1]$	Input-variation weights under low wind speed
q_{high}	$[1.0 \times 10^{-4}, 1.0 \times 10^8]$	State/output weights under high wind speed
p_{high}	$[1.0 \times 10^7, 5.0 \times 10^1]$	Input-variation weights under high wind speed
Q	$\text{diag}(1.0142, 1.0779 \times 10^{-4}, 5.0881 \times 10^{-10})$	Process-noise covariance
R	$\text{diag}(1.0142, 1.0779 \times 10^{-4}, 5.0881 \times 10^{-10})$	Measurement-noise covariance
μ_a	80	Residual χ^2 detection threshold
$\bar{\Delta}$	0.10	Bound of proportional FDI magnitude
N_{MC}	50	Number of Monte Carlo trials

At the communication layer, FDI attacks are introduced into the S-E channel according to the attack model established above to simulate networked environments in which data tampering occurs. In the revised validation, the attacked measurement follows

$$y^a(t_k) = Cx(t_k) + n(t_k) + \vartheta(t_k)a(t_k), \quad (85)$$

where the injected proportional FDI signal is selected as

$$a(t_k) = \Delta(t_k)Cx(t_k), \quad \Delta(t_k) = 0.1 \sin(t_k). \quad (86)$$

This construction produces a bounded time-varying measurement-side attack and is consistent with the proportional FDI model used in the preceding theoretical analysis.

The attack occurrence process is modeled by a Bernoulli random sequence, as specified in (11), which characterizes the probabilistic occurrence of FDI attacks. The parameter $\bar{\theta}$ denotes the occurrence probability of FDI attacks and is used to characterize attack intensity under different network conditions. For illustration, a typical FDI attack sequence is shown in Figure 2, indicating that attacks occur randomly along the time axis.

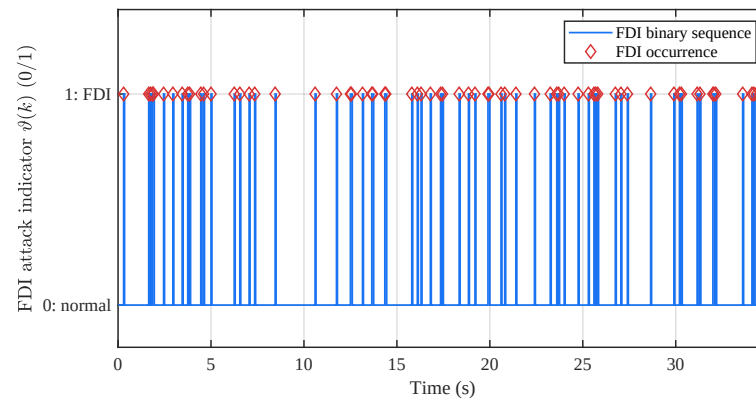


Figure 2. Schematic illustration of FDI attacks.

4.2. Simulation Results

To evaluate the performance of the resilient state estimator under FDI attacks, representative simulations are first conducted. The comparison between the true and estimated system states is shown in Figure 3. In the presence of simultaneous FDI attacks and noise, the resilient state estimator still tracks the true system states, and the estimated trajectories remain broadly consistent with the trends of the true states. When the system states vary rapidly, the estimates respond promptly and approach the true values, indicating that the attack-detection-based EKF maintains effective tracking during transient dynamics. At certain instants, the estimates exhibit transient deviations owing to the combined effect of consecutive short-term attacks and relatively strong measurement noise. This occurs because FDI attacks introduce biased measurements, and when abnormal measurements are detected, the filter relies on model prediction for state updating. Once the attacks cease and valid measurements are again accepted by the detection mechanism, the filter resumes measurement correction, and the posterior estimation error decreases rapidly and reconverges near the true states. These results indicate that the proposed estimator provides disturbance-rejection and recovery capability while maintaining estimation accuracy under random attacks.

To further evaluate the posterior error characteristics of the resilient state estimator, the posterior estimation error trajectories under FDI attacks are plotted in Figure 4. The results show that, under simultaneous FDI attacks and multiple disturbances, the posterior estimation error remains within a finite range and does not diverge over time, which is consistent with the stability property established above. Although the error may increase temporarily under consecutive attacks or strong disturbances, its magnitude remains bounded and decreases rapidly after reliable measurements are restored. This behavior indicates that the residual-based χ^2 attack detection mechanism can provide residual information and suppress detected abnormal measurements, while the modified EKF update maintains estimation continuity through model prediction when measurements are unreliable. Thus, error accumulation and divergence are avoided. The simulation results are consistent with the theoretical boundedness of the posterior estimation error and further support the reliability of the proposed resilient estimator under FDI attacks.

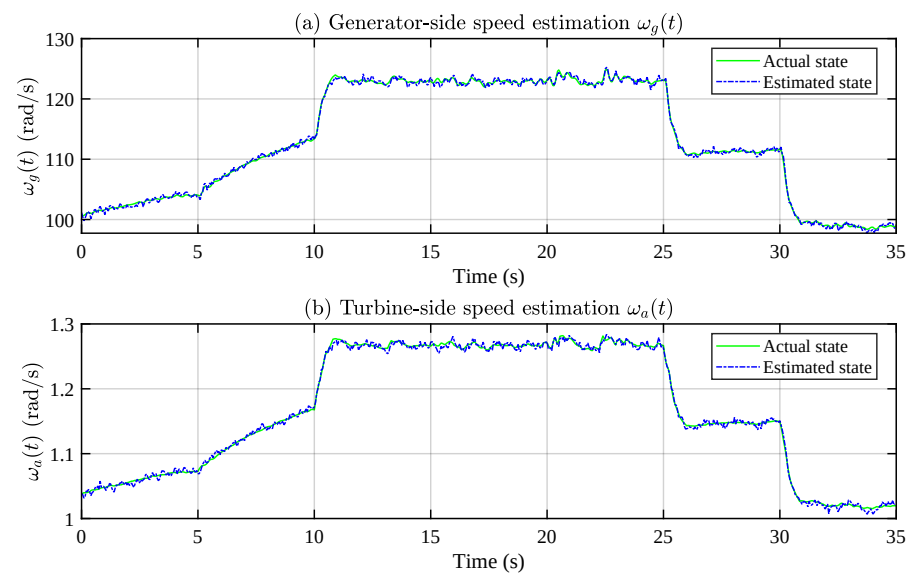


Figure 3. True and estimated state trajectories of EKF-RLMPC under FDI attacks.

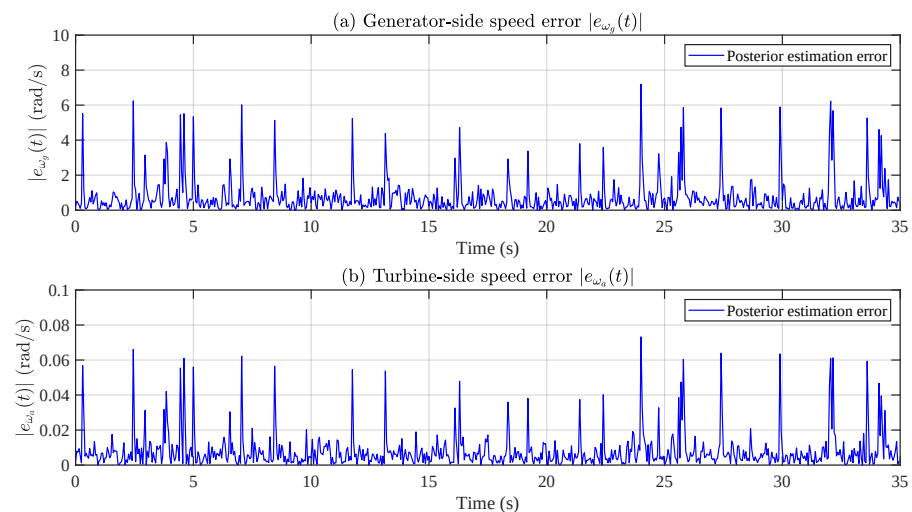


Figure 4. Posterior estimation error trajectories of EKF-RLMPC under FDI attacks.

To examine sensitivity to attack intensity, three FDI attack probabilities are considered: $\bar{\vartheta} = 0.05$, $\bar{\vartheta} = 0.10$, and $\bar{\vartheta} = 0.15$. The resulting state, input, and output-power responses are shown in Figures 5 and 6. A larger $\bar{\vartheta}$ introduces more visible fluctuations and slightly slower settling because a higher number of corrupted measurements enter the estimator-detection loop. Even in the most aggressive case, however, the trajectories remain bounded and return to the admissible operating region, which supports the resilience of the EKF-RLMPC scheme against measurement-side attacks.

The corresponding cost behavior is consistent with the state and power trajectories: increasing the attack probability moderately degrades the closed-loop response, but the degradation remains bounded. Since the controller is updated periodically at every sampling instant, the computational effort is mainly determined by the RLMPC optimization procedure rather than by the random occurrence probability of FDI attacks. The secure and attacked cases are further compared. As shown in Figure 7, secure communication gives faster convergence and smoother state evolution. When FDI attacks are injected, the responses contain additional oscillations and require a longer settling interval, while the input and output-power profiles in Figure 8 remain within acceptable operating ranges.

The comparison confirms that corrupted measurements degrade transient behavior but do not destabilize the closed-loop system under the proposed estimator-controller structure.

To provide a direct interpretation of detection performance for the representative FDI case with $\bar{\vartheta} = 0.15$, a single-run test with the chi-square threshold $\mu_a = 7$ was analyzed. Over 700 control steps, 89 attack steps occurred, giving an actual attack rate of 0.1271. Among these actual attacks, 17 attack steps were not detected, corresponding to a missed detection rate (MDR) of 0.1910. Meanwhile, 22 normal steps were incorrectly flagged as attacks, giving a false alarm rate (FAR) of 0.0360. These results indicate that the reduced detection threshold improves sensitivity to FDI attacks and lowers the missed-detection level, although a limited number of false alarms is introduced.

Figure 9 visualizes the Monte Carlo envelope of the three state trajectories under $\bar{\vartheta} = 0.05$. The gray curves denote individual Monte Carlo trials, the shaded regions represent the mean $\pm$ standard deviation bands, and the solid curves denote the mean trajectories. Although some trajectories exhibit transient deviations due to random FDI attacks and detection errors, all three states remain bounded and follow consistent trends around their mean responses. This supports the practical boundedness of the closed-loop response under stochastic measurement-side attacks.

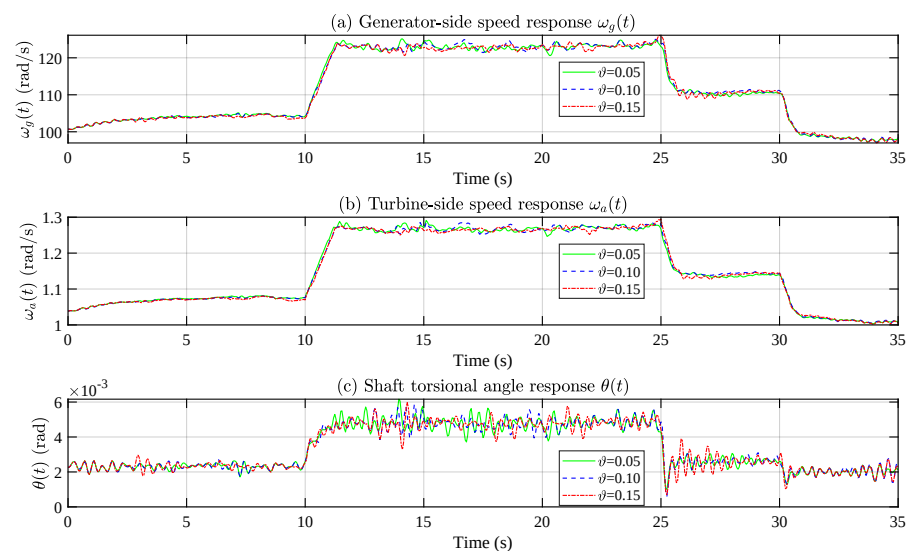


Figure 5. State trajectories of EKF-RLMPC under different FDI attack probabilities.

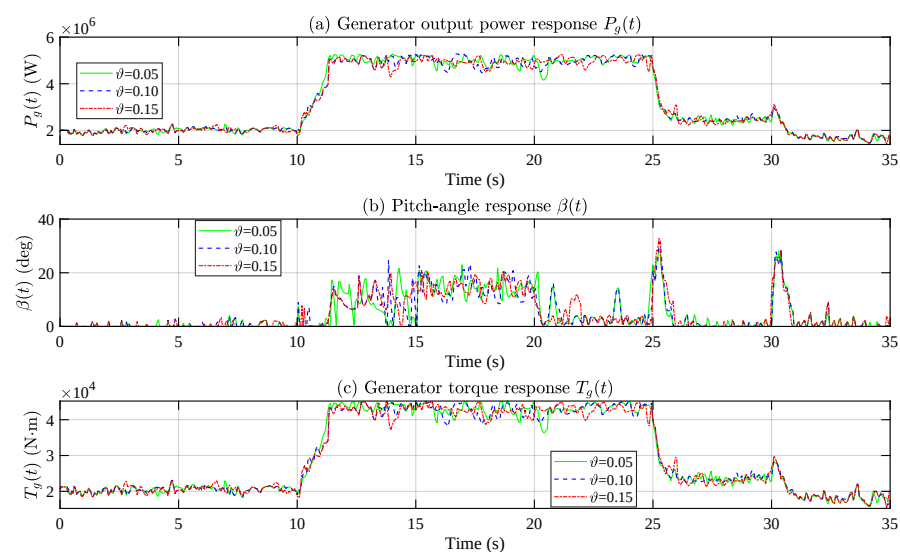


Figure 6. Input and output power trajectories of EKF-RLMPC under different FDI attack probabilities.

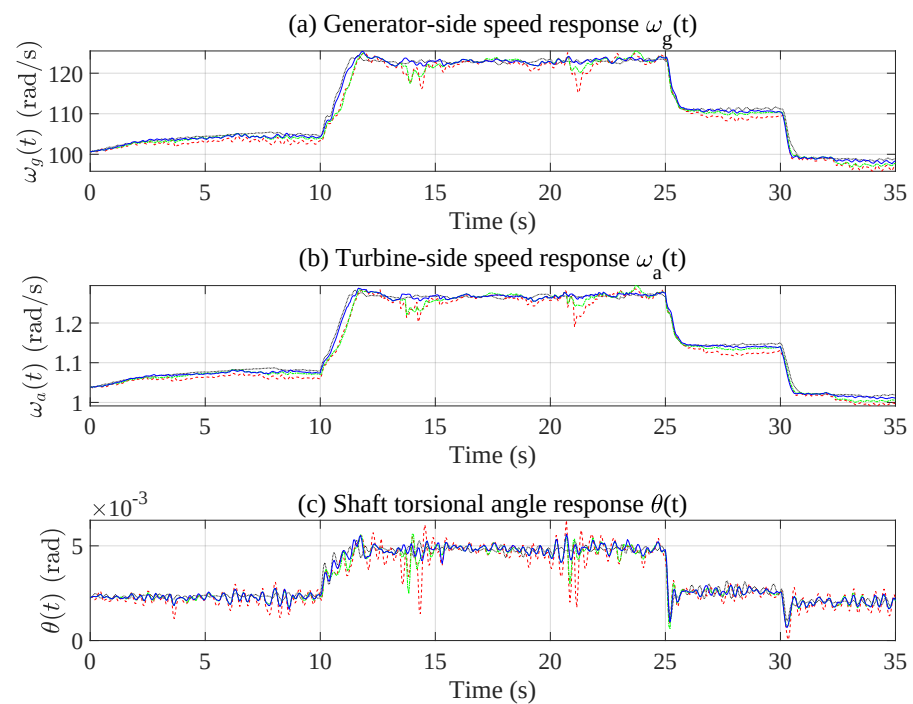


Figure 7. State trajectories of EKF-RLMPC under secure communication and FDI attacks. Line styles: black dotted line, attack-free case; red dashed line, measurement-based RLMPC; green dash-dotted line, EKF-RLMPC without χ^2 detection; blue solid line, proposed EKF- χ^2 -RLMPC.

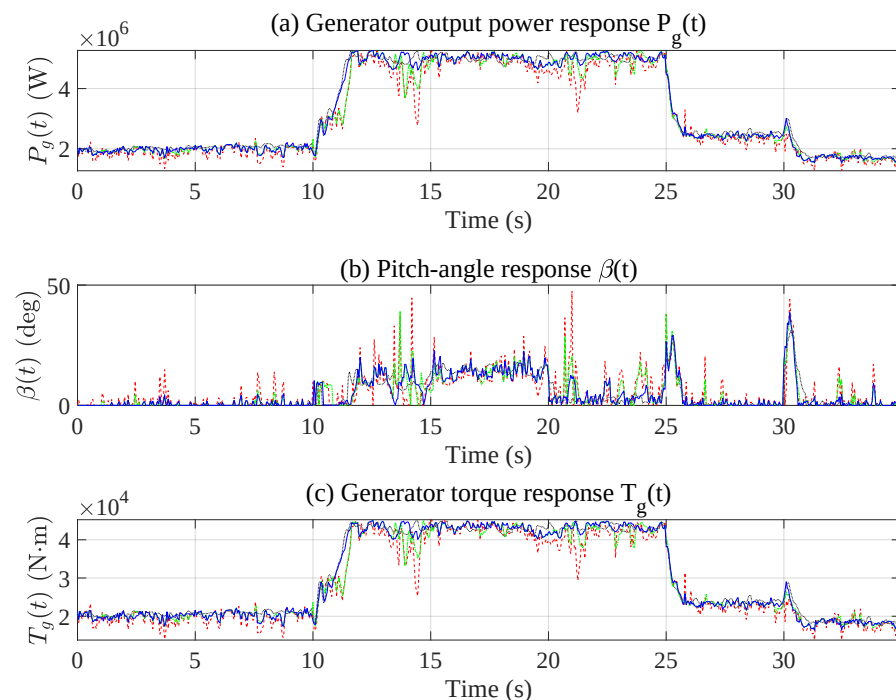


Figure 8. Input and output power trajectories of EKF-RLMPC under secure communication and FDI attacks. Line styles: black dotted line, attack-free case; red dashed line, measurement-based RLMPC; green dash-dotted line, EKF-RLMPC without χ^2 detection; blue solid line, proposed EKF- χ^2 -RLMPC.

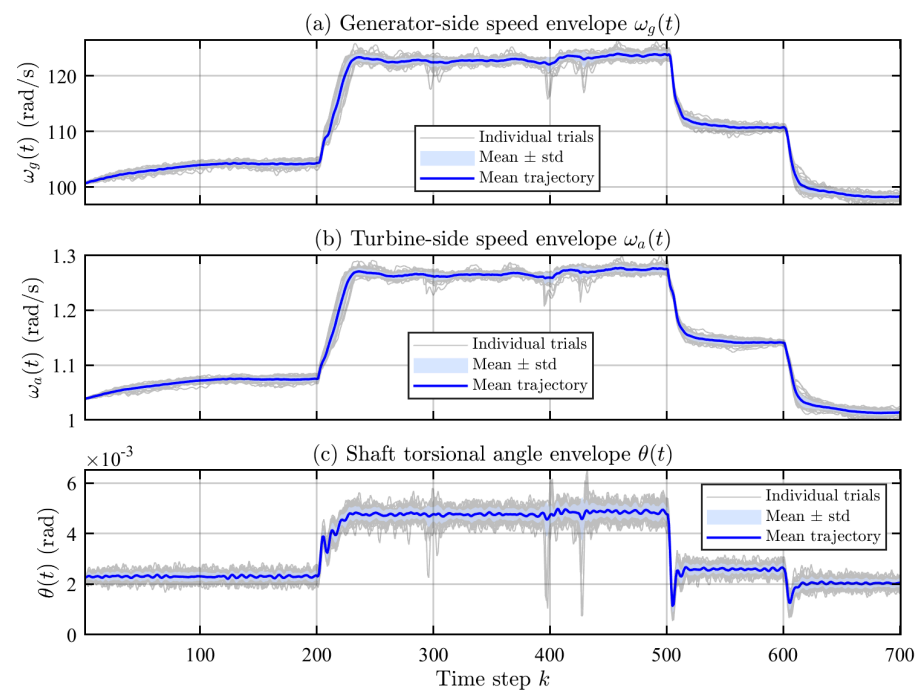


Figure 9. Monte Carlo envelopes of the three state trajectories under $\bar{\vartheta} = 0.05$ over 50 independent trials. The shaded bands denote the mean $\pm$ standard deviation ranges, the gray curves denote individual trials, and the solid curves denote the mean trajectories.

To demonstrate the advantage of the complete EKF- χ^2 -RLMPC structure, ablation-type baseline comparisons were also conducted under $\bar{\vartheta} = 0.15$. The first baseline is a measurement-based RLMPC scheme, which directly uses attacked and noisy measurements as the feedback signal. The second baseline is an EKF-RLMPC scheme without χ^2 detection, where the EKF always applies the measurement correction and does not suppress potentially corrupted measurements. The comparison results are summarized in Table 3.

Table 3. Comparisons under $\bar{\vartheta} = 0.15$ over 50 Monte Carlo trials.

Method	State RMSE	Estimation/Measurement RMSE	IAE
Proposed EKF- χ^2 -RLMPC	5.013 ± 0.132	1.812 ± 0.236	79.868 ± 5.502
Measurement-based RLMPC	5.471 ± 0.167	3.177 ± 0.168	106.616 ± 6.735
EKF-RLMPC without χ^2 detection	5.166 ± 0.114	2.292 ± 0.154	88.506 ± 5.455

As shown in Table 3, the proposed EKF- χ^2 -RLMPC achieves the lowest state RMSE, estimation RMSE, and IAE among the three schemes. Compared with the measurement-based RLMPC, the proposed method reduces the state RMSE by approximately 8.37%, the estimation/measurement RMSE by 42.96%, and the IAE by 25.09%. Compared with the EKF-RLMPC without χ^2 detection, the proposed method reduces the state RMSE by 2.97%, the estimation RMSE by 20.92%, and the IAE by 9.76%. These results indicate that the improvement is not solely due to the use of the RLMPC controller, but also to the attack-aware EKF correction mechanism driven by the residual-based χ^2 detector.

5. Conclusions

This paper investigated the secure predictive control problem for wind power systems subject to stochastic disturbances and FDI attacks. An integrated EKF- χ^2 -RLMPC framework is developed. A residual-based χ^2 detector is designed to evaluate the credibility of received measurements. An EKF estimator is proposed to reconstruct the system state under noisy and possibly corrupted measurements. An RLMPC controller is designed to

compute the control input at every sampling instant using the attack-aware state estimate. Compared with directly using raw measurements for predictive control, the proposed framework couples attack detection, state estimation, and resilient predictive optimization within a unified secure-control structure for wind power systems. Simulation studies verified the effectiveness of the proposed method under stochastic FDI attacks.

Nevertheless, this work still has several limitations. The considered FDI attacks are bounded stochastic measurement attacks, while fully stealthy, coordinated, and model-aware attacks may require more advanced detection and estimation mechanisms. The computational burden is mainly determined by the repeated solution of the RLMPC optimization problem at each sampling instant, and real-time implementation for large-scale wind farms with multiple turbines, communication delays, and distributed sensing infrastructure requires further investigation. Future work will consider measured wind-farm data, hardware-in-the-loop validation, distributed wind-farm control, and advanced resilient estimation methods for more sophisticated cyber-attack scenarios.

Author Contributions: Conceptualization, N.L. and L.Z.; methodology, N.L.; software, N.L.; validation, N.L. and L.Z.; formal analysis, N.L.; investigation, N.L.; resources, L.Z.; data curation, N.L.; writing—original draft preparation, N.L.; writing—review and editing, N.L. and L.Z.; visualization, N.L.; supervision, L.Z.; project administration, L.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding. The APC was funded by the authors.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Lu, P.; Zhang, N.; Ye, L.; Du, E.; Kang, C. Advances in model predictive control for large-scale wind power integration in power systems. *Adv. Appl. Energy* **2024**, *14*, 100177. <https://doi.org/10.1016/j.adapen.2024.100177>.
2. Quan, J.; Zhang, L.; Li, J. Event-Triggered Lyapunov-Based Model Predictive Control for Wind Energy Systems With Measurement Delays. *Int. J. Adapt. Control Signal Process.* **2025**, *39*, 2524–2538. <https://doi.org/10.1002/acs.4065>.
3. Ali, S.W.; Verma, A.K.; Terriche, Y.; Sadiq, M.; Su, C.L.; Lee, C.H.; Elsis, M. Finite-Control-Set Model Predictive Control for Low-Voltage-Ride-Through Enhancement of PMSG Based Wind Energy Grid Connection Systems. *Mathematics* **2022**, *10*, 4266. <https://doi.org/10.3390/math10224266>.
4. Elsis, M.; Tran, M.Q.; Hasanien, H.M.; Turkey, R.A.; Albalawi, F.; Ghoneim, S.S.M. Robust Model Predictive Control Paradigm for Automatic Voltage Regulators against Uncertainty Based on Optimization Algorithms. *Mathematics* **2021**, *9*, 2885. <https://doi.org/10.3390/math9222885>.
5. Li, G.; Zeng, J.; Liu, J. Effluent Quality-Aware Event-Triggered Model Predictive Control for Wastewater Treatment Plants. *Mathematics* **2023**, *11*, 3912. <https://doi.org/10.3390/math11183912>.
6. Hu, Z.; Su, R.; Ling, K.V.; Guo, Y.; Ma, R. Resilient event-triggered MPC for load frequency regulation with wind turbines under false data injection attacks. *IEEE Trans. Autom. Sci. Eng.* **2023**, *21*, 7073–7083. <https://doi.org/10.1109/TASE.2023.3337006>.
7. Yang, J.; Zhong, Q.; Shi, K.; Zhong, S. Co-design of observer-based fault detection filter and dynamic event-triggered controller for wind power system under dual alterable DoS attacks. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1270–1284. <https://doi.org/10.1109/TIFS.2022.3160355>.
8. Zhang, X.; Liu, Z.; Xiao, F.; Wei, B.; Fang, F.; Qin, S.; Zhou, C. Dynamic Event-Triggered Optimal Rotor Speed Tracking Control and Co-Simulation for Wind Turbines Under Hybrid Attacks. In *Proceedings of the 2025 IEEE 4th International Conference on Industrial Electronics for Sustainable Energy Systems (IESES)*; IEEE: Piscataway, NJ, USA, 2025; pp. 280–287.
9. Zhai, M.; Yang, T.; Wu, Q.; Guo, S.; Pang, R.; Sun, N. Extended Kalman filtering-based nonlinear model predictive control for underactuated systems with multiple constraints and obstacle avoidance. *IEEE Trans. Cybern.* **2024**, *55*, 369–382. <https://doi.org/10.1109/TCYB.2024.3488371>.
10. Honarbari, A.; Najafi-Shad, S.; Saffari Pour, M.; Ajarostaghi, S.S.M.; Hassannia, A. MPPT improvement for PMSG-based wind turbines using extended Kalman filter and fuzzy control system. *Energies* **2021**, *14*, 7503. <https://doi.org/10.3390/en14227503>.

11. ur Rehman, A.; Ali, N.; Khan, O.; Pervaiz, M. A disturbance observer based sliding mode control for variable speed wind turbine. *IETE J. Res.* **2022**, *68*, 1823–1830. <https://doi.org/10.1080/03772063.2019.1676661>.
12. Liu, X.; Feng, L.; Kong, X.; Guo, S.; Lee, K.Y. Tube-based stochastic model predictive control with application to wind energy conversion system. *IEEE Trans. Control Syst. Technol.* **2023**, *31*, 2173–2187. <https://doi.org/10.1109/TCST.2023.3291531>.
13. Kim, M.; Jang, M.; Park, S. A data-driven model predictive control for wind farm power maximization. *IEEE Access* **2024**, *12*, 90670–90683. <https://doi.org/10.1109/ACCESS.2024.3420872>.
14. Huang, R.; Patwardhan, S.C.; Biegler, L.T. Robust stability of nonlinear model predictive control with extended Kalman filter and target setting. *Int. J. Robust. Nonlinear Control* **2013**, *23*, 1240–1264. <https://doi.org/10.1002/rnc.2817>.
15. Chen, Y.; Li, T.; Long, Y.; Bai, W. Attacks Detection and Security Control for Cyber-Physical Systems under False Data Injection Attacks. *J. Frankl. Inst.* **2023**, *360*, 10476–10498. <https://doi.org/10.1016/j.jfranklin.2023.07.020>.
16. Suo, Y.; Chai, R.; Chai, S.; Farhan, I.M.D.; Xia, Y.; Liu, G.P. Attack Detection and Secure State Estimation of Collectively Observable Cyber-Physical Systems Under False Data Injection Attacks. *IEEE Trans. Autom. Control* **2024**, *69*, 2067–2074. <https://doi.org/10.1109/TAC.2023.3316160>.
17. Hu, S.; Chen, X.; Li, J.; Xie, X. Observer-based resilient controller design for networked stochastic systems under coordinated DoS and FDI attacks. *IEEE Trans. Control Netw. Syst.* **2023**, *11*, 890–901. <https://doi.org/10.1109/TCNS.2023.3314578>.
18. Duo, W.; Zhou, M.; Abusorrah, A. A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 784–800. <https://doi.org/10.1109/JAS.2022.105548>.
19. Lian, Z.; Shi, P.; Chen, M. A survey on cyber-attacks for cyber-physical systems: Modeling, defense, and design. *IEEE Internet Things J.* **2024**, *12*, 1471–1483.
20. Zhang, Z.; Feng, X. Performance analysis of chi-square detection for false data injection attack. In *Proceedings of the 2023 3rd International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT)*; IEEE: Piscataway, NJ, USA, 2023; pp. 560–564. <https://doi.org/10.1109/ICEEMT59522.2023.10263144>.
21. Wang, P.; Zhang, R.; He, X. New Approaches to Detection and Secure Control for Cyber-Physical Systems Against False Data Injection Attacks. *Int. J. Control Autom. Syst.* **2025**, *23*, 332–345. <https://doi.org/10.1007/s12555-024-0352-z>.
22. Zhao, S.; Yang, Q.; Cheng, P.; Deng, R.; Xia, J. Adaptive resilient control for variable-speed wind turbines against false data injection attacks. *IEEE Trans. Sustain. Energy* **2022**, *13*, 971–985. <https://doi.org/10.1109/TSTE.2022.3141766>.
23. Xu, D.; Liu, Y.; Lee, S. Secure Control for T-S Fuzzy Wind Turbine Systems Under Hybrid Cyberattacks via an Adaptive Memory Event-Triggered Mechanism. *IEEE Trans. Fuzzy Syst.* **2025**, *33*, 1475–1487. <https://doi.org/10.1109/TFUZZ.2025.3525778>.
24. Wu, H.; Badihi, H.; Xue, Y.; Vilkko, M. Smart coordinated cyber-attacks on wind turbines: From detection to identification via machine learning. *Sustain. Energy Grids Netw.* **2025**, *43*, 101775. <https://doi.org/10.1016/j.segan.2025.101775>.
25. Scibilia, A.; Garraffa, G.; Lai, Q.; Fortuna, L. Identity Between Bounded Real and Positive Real Characteristic Values Through the Scattering Relation. *IEEE Access* **2026**, *14*, 58248–58261. <https://doi.org/10.1109/ACCESS.2026.3681180>.
26. Zhang, J.; Liu, S.; Liu, J. Economic model predictive control with triggered evaluations: State and output feedback. *J. Process Control* **2014**, *24*, 1197–1206. <https://doi.org/10.1016/j.jprocont.2014.03.009>.
27. Liu, S.; Liu, J. Distributed lyapunov-based model predictive control with neighbor-to-neighbor communication. *AIChE J.* **2014**, *60*, 4124–4133. <https://doi.org/10.1002/aic.14579>.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.