Tube Model Predictive Control Based Cyber-attack-resilient Optimal Voltage Control Strategy in Wind Farms

Zhenming Li, Minghao Wang, *Senior Member*, *IEEE*, *Senior Member*, *CSEE*, Yunfeng Yan, Donglian Qi, *Senior Member*, *IEEE*, *Senior Member*, *CSEE*, Zhao Xu, *Senior Member*, *IEEE*, *Senior Member*, *CSEE*, Jianliang Zhang, and Zezhou Wang

***Abstract*—Optimal voltage controls have been widely applied in wind farms to maintain voltage stability of power grids. In order to achieve optimal voltage operation, authentic grid information is widely needed in the sensing and actuating processes. However, this may induce system vulnerable to malicious cyber-attacks. To this end, a tube model predictive control-based cyber-attack-resilient optimal voltage control method is proposed to achieve voltage stability against malicious cyber-attacks. The proposed method consists of two cascaded model predictive controllers (MPC), which outperform other peer control methods in effective alleviation of adverse effects from cyber-attacks on actuators and sensors of the system. Finally, efficiency of the proposed method is evaluated in sensor and actuator cyber-attack cases based on a modified IEEE 14 buses system and IEEE 118 buses system.**

***Index Terms*—Attack-resilient control, optimal voltage control, tube-based model predictive control, wind farm-connected power system.**

I. Introduction

THE integration of eco-friendly renewable energy sources in power grids can benefit decarbonization of energy systems effectively. However, it is challenging to tame embedded intermittency of renewables to fulfil conventional grid codes on efficiency, security, and stability [1]. To meet this challenge, Information and Communication Technology (ICT), Supervisory Control and Data Acquisition (SCADA) systems, and massive sensors/actuators have been used extensively in power grids. Exploitation of advanced information and communication technology upgrades modern power grids towards a cyber-physical system (CPS) [2], termed a cyber-physical power systems (CPPS).

The cyber security of CPPS has attracted extensive attention [3]–[5]. In CPPS, downstream grids are more vulnerable to cyber-attacks, imposing critical threats to safe power grid operations [6]. So far, cyber-attacks have caused several power accidents all over the world [7], [8], and have been proven sufficiently complex attacks can lead to catastrophic consequences such as overvoltage/undervoltage, equipment damage, cascading failures [9], distributed energy resources (DER) disconnection, etc [10].

Power grids connected with wind farms, as typical CPPSs, have received extensive attention [11]. Their cyber security is a concern for both academia and industry. Generally, there are two ways to improve robustness of the system under cyber-attacks: one is to design data encryption transmission laws, and the other is to design attack-resilient control strategies. This paper focuses on the latter. Recently, some relevant works have been reported. For example, an attack-mitigation strategy based on forecast information is proposed in [12] to deal with cyber-attacks on a wind farm SCADA system. The authors in [13] develop an adaptive resilient control strategy to improve the attack resiliency of the wind turbine control system. The time delay problem of distributed CPPS is discussed in [14], which proposes a method to improve system robustness from the perspective of communication link planning. The development of attack-resilient algorithms leads the strategies of dealing with cyber-attacks from recognition and detection to mitigation and elimination control.

Voltage control is an important part to maintain grid voltage stability in the presence of renewable energy. Analysis and mitigation of the impacts of cyber-attack have also received wide attention. It has been reported that a false data injection attack (FDIA) can corrupt automatic voltage control (AVC) [15]. Voltage control problems induced by different attacks have been well studied. Typically, Petri Net and self-organizing network structures are adopted in [16], [17] to mitigate impacts on voltage control from malicious cyber-attacks. Specifically, in [16], Petri Net is used to describe the influence of attacks on power systems, which contributes to event-triggered mechanism design and suppression of voltage fluctuation. In [17], a self-organizing network structure is used to maintain voltage stability of distribution networks against multiple attack formats and increasing numbers of attackers.

Manuscript received December 26, 2021; revised March 1, 2022; accepted April 13, 2022. Date of online publication March 3, 2023; date of current version Feberuary 14, 2024. This work was supported by the National Natural Science Foundation of China (U1909201) and the Hong Kong Polytechnic University Research Program (SB2D).

Z. M. Li, J. L. Zhang, Y. F. Yan and D. L. Qi are with the College of Electrical Electronic Engineering, Zhejiang University, Hangzhou 310058, China.

M. H. Wang (corresponding author, email: minghao.wang@polyu.edu.hk) and Z. Xu are with the Department of Electrical Engineering, The Hong Kong Polytechnic University, Kowloon, Hong Kong, China.

Z. Z. Wang is with Haiyan power supply company of State Grid Zhejiang Electric Power Co., Ltd, Hangzhou, China.

DOI: 10.17775/CSEEJPES.2021.09490

Different from current research work, in [18], the authors mainly focus on cyber-attacks on voltage control parameters rather than communication networks, in which a countermeasure of controlled switching units is proposed to handle such attacks. In addition to centralized control structure, distributed control schemes are adopted to address voltage control problems of renewable-integrated power grids under various network attacks [19]–[21]. This method is commonly used to eliminate adverse effects on renewable energy.

However, to the best of our knowledge, there is no theoretical foundation to explicitly model the impact of a cyber-attack on grid voltage optimization processes rather than control processes in wind power-integrated grids. Moreover, the effective approach for eliminating the cyber-attacks influence on control optimality is painfully missing. To fill this research gap, a tube model predictive control-based cyber-attack-resilient optimal voltage control method is proposed in this paper.

The tube-based model predictive control (TMPC) has been applied in several areas to address optimal control problems incurred with disturbance. A control theory solution for hybrid electric vehicles' energy management is proposed in [22], [23] to deal with future torque demand and uncertain vehicle speed. These researches discussed the application of tube-based MPC on suboptimal control of bus voltage in active distribution networks. In [24], tube-based MPC is reported to address the problem of grid frequency regulation when electric vehicles are connected. In [25], [26], the energy optimization management method of microgrids with energy storage based on tube-based MPC is discussed. In summary, research on using tube-based MPC for addressing optimal voltage control problems under cyber-attacks is still in its infancy.

Based on tube-based model predictive control (TMPC) theory, two cascaded MPCs are designed to eliminate the influence of cyber-attacks on optimization results. Specifically, nominal MPC is used to generate the optimized reference value in absence of cyber-attacks. Ancillary MPC is used to maintain control variables within the vicinity of obtained optimal reference value against cyber-attacks.

The rest of the paper is organized as follows: a dynamic model of wind farms and optimal voltage control problem are elaborated in Section II. Impact of cyber-attacks on optimal voltage control process is analyzed in Section III. The relevant theory of TMPC is provided in Section IV. An attack-resilient optimal voltage control algorithm for wind farms based on TMPC is discussed in Section V. A verification analysis by case studies and conclusions of our work are provided in Sections VI and VII, respectively.

II. Preliminaries on the System Model

In this section, the dynamic model of wind farms without malicious cyber-attacks is formulated, and the optimal voltage control problem is analyzed.

A. Discrete-time Control of Wind Farms without Cyber-Attacks

A first-order wind farm model is commonly used in voltage control and optimization of wind farms based on model predictive control and distributed optimization algorithms. Based on [27]–[29], wind farms are mainly comprised of (i) wind turbine generators (WTGs) and (ii) stochastic voltage compensators or generators (SVCs/SVGs). Each part is modeled as a first-order function according to conventional transient models in this study.

Dynamic models of WTGs and SVCs/SVGs can be expressed as follows, respectively [30]:

$$\Delta\dot{Q}_{\mathrm{W}} = -\frac{1}{T_{\mathrm{W}}}\Delta Q_{\mathrm{W}} + \frac{1}{T_{\mathrm{W}}}\Delta Q_{\mathrm{W}}^{\mathrm{ref}} \tag{1}$$

$$\begin{bmatrix}\Delta\dot{Q}_{\mathrm{S}}\\ \Delta\dot{V}_{\mathrm{int}}\end{bmatrix} = \boldsymbol{A}_{\mathrm{S}}\begin{bmatrix}\Delta Q_{\mathrm{S}}\\ \Delta V_{\mathrm{int}}\end{bmatrix} + \boldsymbol{E}_{\mathrm{S}}\Delta Q_{\mathrm{W}} + \boldsymbol{B}_{\mathrm{S}}\Delta V_{\mathrm{S}}^{\mathrm{ref}} \tag{2}$$

where

$$\begin{cases}\boldsymbol{A}_{\mathrm{S}} = \begin{bmatrix}-\frac{1}{T_{\mathrm{S}}}\left(1+K_{\mathrm{P}}\frac{\partial|V_{\mathrm{S}}|}{\partial Q_{\mathrm{S}}}\right) & \frac{K_{\mathrm{I}}}{T_{\mathrm{S}}}\\ -\frac{\partial|V_{\mathrm{S}}|}{\partial Q_{\mathrm{S}}} & 0\end{bmatrix}\\ \boldsymbol{E}_{\mathrm{S}} = \begin{bmatrix}-\frac{K_{\mathrm{P}}}{T_{\mathrm{S}}}\frac{\partial|V_{\mathrm{S}}|}{\partial Q_{\mathrm{W}}}\\ -\frac{\partial|V_{\mathrm{S}}|}{\partial Q_{\mathrm{W}}}\end{bmatrix}\\ \boldsymbol{B}_{\mathrm{S}} = \begin{bmatrix}\frac{K_{\mathrm{P}}}{T_{\mathrm{S}}}\\ 1\end{bmatrix}\end{cases} \tag{3}$$

In (1) and (3), T_{W} and T_{S} denote the time constant of WTGs and SVC/SVG, respectively. ΔQ_{W} denotes the changed reactive power of WTGs, and $\Delta Q_{\mathrm{W}}^{\mathrm{ref}}$ is the reference of ΔQ_{W}. K_{P} and K_{I} represent the proportional and integral gains of the SVC/SVG PI controller, respectively. $\frac{\partial|V_{\mathrm{S}}|}{\partial Q_{\mathrm{S}}}$ and $\frac{\partial|V_{\mathrm{S}}|}{\partial Q_{\mathrm{W}}}$ are the sensitivity coefficients of reactive power outputs of WTGs and SVC/SVG [31].

Based on (1) and (2), a dynamic model of wind farms without malicious cyber-attacks can be formulated as (4).

$$\dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u} \tag{4}$$

where

$$\begin{aligned}\boldsymbol{x} = \big[&\Delta Q_{\mathrm{S}_1}, \Delta V_{\mathrm{int}_1}, \cdots, \Delta Q_{\mathrm{S}_{N_{\mathrm{S}}}}, \Delta V_{\mathrm{int}_{N_{\mathrm{S}}}}, \Delta Q_{\mathrm{S}_1},\\ &\cdots, \Delta Q_{\mathrm{W}_{N_{\mathrm{W}}}}\big]^{\mathrm{T}}\end{aligned} \tag{5}$$

$$u = \left[\Delta V_{\mathrm{S}_1}^{\mathrm{ref}}, \cdots, \Delta V_{\mathrm{S}_{N_{\mathrm{S}}}}^{\mathrm{ref}}, \Delta Q_{\mathrm{W}_1}^{\mathrm{ref}}, \cdots, \Delta Q_{\mathrm{W}_{N_{\mathrm{W}}}}^{\mathrm{ref}}\right]^{\mathrm{T}} \tag{6}$$

and

$$\boldsymbol{A} = \begin{bmatrix}\boldsymbol{A}_{\mathrm{S}_1} & \cdots & 0 & \boldsymbol{E}_{\mathrm{S}_1} & \cdots & 0\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 0 & \cdots & \boldsymbol{A}_{\mathrm{S}_{N_{\mathrm{S}}}} & 0 & \cdots & \boldsymbol{E}_{\mathrm{S}_{N_{\mathrm{W}}}}\\ 0 & \cdots & 0 & -\frac{1}{T_{\mathrm{W}_1}} & \cdots & 0\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 0 & \cdots & 0 & 0 & \cdots & -\frac{1}{T_{\mathrm{W}_{N_{\mathrm{W}}}}}\end{bmatrix} \tag{7}$$

$$\boldsymbol{B} = \begin{bmatrix}\boldsymbol{B}_{\mathrm{S}_1} & \cdots & 0 & 0 & \cdots & 0\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 0 & \cdots & \boldsymbol{B}_{\mathrm{S}_{N_{\mathrm{S}}}} & 0 & \cdots & 0\\ 0 & \cdots & 0 & \frac{1}{T_{\mathrm{W}_1}} & \cdots & 0\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 0 & \cdots & 0 & 0 & \cdots & \frac{1}{T_{\mathrm{W}_{N_{\mathrm{W}}}}}\end{bmatrix} \tag{8}$$

According to [32], (4) can be transformed into a discrete-time model with sampling time ΔT_{d},

$$\boldsymbol{x}(k+1)=\boldsymbol{A}_{\mathrm{d}}\boldsymbol{x}(k)+\boldsymbol{B}_{\mathrm{d}}\boldsymbol{u}(k) \tag{9}$$

where $\boldsymbol{A}_{\mathrm{d}}=\mathrm{e}^{\boldsymbol{A}\Delta T}\cong\boldsymbol{I}+\boldsymbol{A}\Delta T$, $\boldsymbol{B}_{\mathrm{d}}=\int_0^{\tau}\mathrm{e}^{\boldsymbol{A}\Delta T}\mathrm{d}\tau\cong\boldsymbol{B}\Delta T$ are the discrete forms of $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively. $\boldsymbol{I}$ is the identity matrix.

B. Objective Function of Wind Farms

The objective function targets minimizing voltage fluctuation at the Point of Connection (POC) and reactive power change of WTGs and SVCs/SVGs per control period considering ramping rates, which can be expressed as (10).

$$\min\|\Delta V_{\mathrm{POC}}\|^2+\sum_{i=1}^{N_{\mathrm{S}}}\|\Delta Q_{\mathrm{S}_i}\|^2+\sum_{i=1}^{N_{\mathrm{W}}}\|\Delta Q_{\mathrm{W}_i}\|^2 \tag{10}$$

where ΔQ_{S_i} and ΔQ_{W_i} are reactive power deviations of SVG and wind turbines, respectively. ΔV_{POC} is the difference between current POC voltage (V_{POC}) and POC voltage reference (the rated voltage). ΔV_{POC} can be expressed as (11).

$$\Delta V_{\mathrm{POC}}=V_{\mathrm{POC}}+\frac{\partial|V_{\mathrm{POC}}|}{\partial Q_{\mathrm{S}}}\Delta Q_{\mathrm{S}}+\frac{\partial|V_{\mathrm{POC}}|}{\partial Q_{\mathrm{W}}}\Delta Q_{\mathrm{W}}-V_{\mathrm{POC}}^{\mathrm{ref}} \tag{11}$$

The reactive power outputs of WTGs and SVCs/SVGs are bounded by (12) and (13).

$$Q_{\mathrm{Smin}}\le Q_{\mathrm{S}}\le Q_{\mathrm{Smax}} \tag{12}$$

$$Q_{\mathrm{Wmin}}\le Q_{\mathrm{W}}\le Q_{\mathrm{Wmax}} \tag{13}$$

III. Cyber-Attacks Against Optimal Control of Wind Farms

The cyber-attacks are considered twofold: 1) Cyber-attacks compromise state estimation of power grids. These attacks mislead operators by polluting state estimates with false data. 2) The cyber-attacks penetrate the cyber system of the wind farm operation system via sensors, actuators, and communication links (see Fig. 1). These attacks tamper control or optimization results by injecting false wind field data.

The attack vector is defined as $\boldsymbol{\alpha}=[\alpha_1,\alpha_2,\cdots,\alpha_{2N_{\mathrm{S}}+N_{\mathrm{W}}}]^{\mathrm{T}}$. It should be noted that due to the existence of the bad data detection function in the power grid, the size of the attack is usually limited from the attacker's perspective [33], [34]. Models of attacks on the aforementioned three parts are modeled hereafter.

A. Cyber-attacks on Sensors

$$\boldsymbol{x}^{\mathrm{a}}=\boldsymbol{x}+\boldsymbol{\alpha} \tag{14}$$

where x is the actual state of the wind farms, and $\boldsymbol{x}^{\mathrm{a}}$ is the attacked state sent to the control center. Dynamics of the wind farm with SVCs/SVGs can be expressed as follows,

$$\dot{\boldsymbol{x}}^{\mathrm{a}}=\boldsymbol{A}\boldsymbol{x}^{\mathrm{a}}+\boldsymbol{B}\boldsymbol{u} \tag{15}$$

B. Cyber-attacks on Actuators

$$\boldsymbol{u}^{\mathrm{a}}=\boldsymbol{u}+\boldsymbol{\alpha} \tag{16}$$

where u is control input without attacks on the wind farms, and

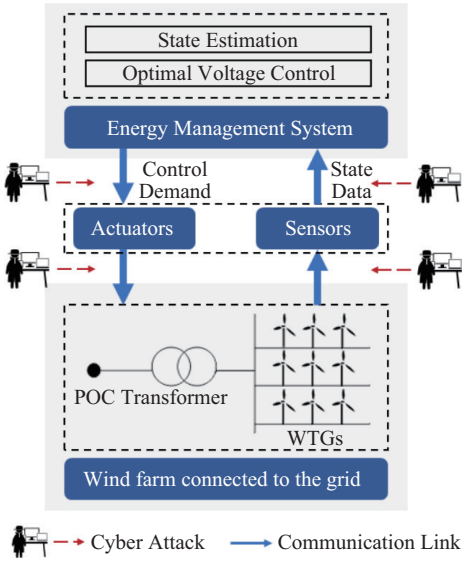

Fig. 1. Location of the attack intrusion.

$\boldsymbol{u}^{\mathrm{a}}$ is the attacked control input dispatched from the control center. Then, the dynamics of the wind farm with SVC/SVG can be expressed as

$$\dot{\boldsymbol{x}}=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{B}\boldsymbol{u}^{\mathrm{a}} \tag{17}$$

C. Cyber-attacks on Communication Links

When cyber-attacks on communication links occur between sensors/actuators and the control center, the FDIA will cause the same effects as the cyber-attacks on sensors/actuators.

The following theorem summarizes the properties of the wind farm under cyber-attacks.

Theorem 1. Suppose the control center dispatches the optimized control instruction based on $\boldsymbol{x}^{\mathrm{a}}$ and $\boldsymbol{u}^{\mathrm{a}}$, and the optimized instructions with and without attacks are $\boldsymbol{u}^{*}$ and $\boldsymbol{u}^{\mathrm{a}*}$, respectively. The cyber-attacks will impose a deviation from the optimal voltage control instructions.

The proof of Theorem 1 is provided in the Appendix.

Theorem 1 explains the impact of cyber-attacks on optimal operation of the grid and wind farms with respect to different locations. From the perspective of attackers, attacks on the voltage optimization process induce more power losses and instabilities. Furthermore, adverse effects caused by such attacks will accumulate in iterative time-receding optimization, eventually causing more losses to the grid.

IV. Tube-based Model Predictive Control

A. Overview of TMPC

TMPC is an effective approach to eliminate the influence of disturbances on the controller. Generally, an uncertain system can be modeled as [35].

$$x_{t+1}=Ax_t+Bu_t+w_t \tag{18}$$

where x represents states of the system, u represents control actions, and w represents disturbances.

TMPC consists of two cascaded MPC controllers, as shown in Fig. 2: 1) nominal MPC controller: to generate a central

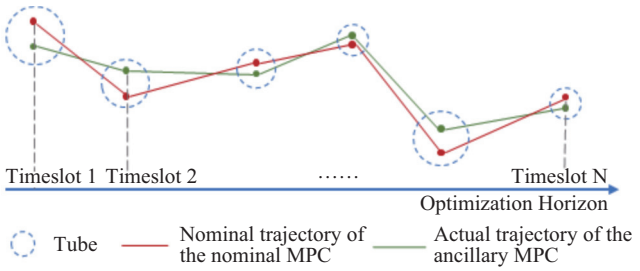

Fig. 2. Diagram of tube-based MPC.

trajectory under tightened constraints; 2) ancillary MPC controller: to guide trajectory under disturbances to converge to the aforementioned central trajectory. The design of these two controllers will be described in the next two parts specifically.

B. Nominal MPC

A nominal system can be obtained from (18) by neglecting the disturbance term w.

$$\bar{\boldsymbol{x}}_{t+1} = \boldsymbol{A}\bar{\boldsymbol{x}}_t + \boldsymbol{B}\bar{\boldsymbol{u}}_t \tag{19}$$

where $\bar{\boldsymbol{x}}_t$ denotes nominal system states and $\bar{\boldsymbol{u}}_t$ represents nominal control actions.

The objective function of this controller is consistent with the original problem to be solved. Constraints of this controller are tightened compared with those of the original problem.

C. Ancillary MPC

The ancillary controller aims to guide trajectory under disturbances to converge to the aforementioned nominal trajectory, namely, to form a 'tube' around the reference.

To achieve this, the ancillary MPC is designed to minimize the deviation of the state variable x and control variable u from nominal trajectories by using (20).

$$\min \sum_{N_x} \mu_x(\boldsymbol{x}_t - \bar{\boldsymbol{x}}_t)^2 + \sum_{N_u} \mu_u(\boldsymbol{u}_t - \bar{\boldsymbol{u}}_t)^2 \tag{20}$$

where N_x and N_u denote the number of state and control variables, respectively. μ_x and μ_u are weights associated with deviation of state and control variables.

Constraints in the ancillary MPC are the same as the original problem, except disturbance w is considered.

V. Tube-based MPC of Wind Farms Considering Malicious Cyber-attack

A. Nominal MPC Design

A nominal MPC controller is designed by neglecting malicious cyber-attacks on actuators and sensors of WTGs and SVCs/SVGs. Without attacks, control input obtained from the nominal MPC controller is disturbance-free control input, leading to the desired state. Based on this assumption, the objective function of the nominal MPC is the same as (4),

$$\begin{aligned}\min &\sum_{t=1}^{N_\mathrm{p}} \|\Delta V_{\mathrm{POC}}(t)\|^2 + \sum_{t=1}^{N_\mathrm{p}}\sum_{i=1}^{N_\mathrm{S}} \|\Delta Q_{\mathrm{S}_i}(t)\|^2 \\ &+ \sum_{t=1}^{N_\mathrm{p}}\sum_{i=1}^{N_\mathrm{W}} \|\Delta Q_{\mathrm{W}_i}(t)\|^2 \end{aligned} \tag{21}$$

where N_p represents prediction times in a prediction period. According to TMPC theory, constraints of the nominal MPC should be tightened by using (22) and (23).

$$(1+\rho_1)Q_{\mathrm{Smin}} \le Q_\mathrm{S} \le (1-\rho_2)Q_{\mathrm{Smax}} \tag{22}$$

$$(1+\rho_1)Q_{\mathrm{Wmin}} \le Q_\mathrm{W} \le (1-\rho_2)Q_{\mathrm{Wmax}} \tag{23}$$

where ρ_1 and ρ_2 are the parameters for tightening constraints. They are chosen by offline Monte Carlo simulations to maintain the robustness of the algorithm [35]. Varying degrees of robustness can be achieved by adjusting these parameters [36]. In the case of Monte Carlo simulations, ρ_1 and ρ_2 are reduced if the constraints of the system are violated. If the constraint is too conservative, these two parameters are increased.

B. Ancillary MPC Design

The ancillary MPC controller will regulate state and control variables of the disturbed systems within the tube, which can be formulated as an optimal tracking problem as (24).

$$\min \sum_{t=1}^{N_\mathrm{q}} \mu_x(\boldsymbol{x}_i - \boldsymbol{x}_i^{\mathrm{ref}})^2 + \mu_u(\boldsymbol{u}_i - \boldsymbol{u}_i^{\mathrm{ref}})^2 \tag{24}$$

where $\boldsymbol{x}_i^{\mathrm{ref}}$ and $\boldsymbol{u}_i^{\mathrm{ref}}$ are references of the state and control variables, derived from the nominal MPC. μ_x and μ_u are weights of state and control variable. N_q represents the prediction period of the ancillary MPC: typically, $N_\mathrm{q} < N_\mathrm{p}$. Associated constraints are (12), (13).

Prediction of the first time slot is fed to the controller as the optimization result, i.e., control demands of the present control period. Then, the prediction period rolls back. New state values are fed to the nominal MPC. New references generated by the nominal MPC will be fed to the ancillary MPC until the optimal control process terminates.

The TMPC control process considering malicious cyber-attacks is shown in Fig. 3.

VI. Simulation Results

The proposed attack-resilient optimal voltage control strategy is validated on the IEEE 14-bus and 118-bus test bench. The wind farm consists of 20 × 5 MW WTGs, and a 10 MW SVG. It is connected to transmission network (IEEE 14-bus system) through a step-up transformer at bus 13, as shown in Fig. 4. The wind farm is connected to the IEEE 118-bus system through a step-up transformer at bus 11. Active power profile of the wind farm can be plotted in Fig. 5 [30].

Two attack scenarios were considered, namely, 1) cyber-attacks on the sensor side. 2) cyber-attacks on the actuator side. Both attacks are launched at $t = 50$ s. Total simulation time is set to be 600 s.

A. Case 1: Sensor Attacks

To evaluate performance of the proposed attack-resilient voltage optimization control, random attacks on sensors are investigated with $\dot{\boldsymbol{x}}^{\mathrm{a}} = \boldsymbol{A}\boldsymbol{x}^{\mathrm{a}} + \boldsymbol{B}\boldsymbol{u}$, where $\boldsymbol{x}^{\mathrm{a}}$ is the state measurement. $\boldsymbol{u}$ is the control input vector.

Simulation results of random attacks on sensors are shown in Figs. 6 and 7. Before the attack occurs (0∼50 s), the reactive

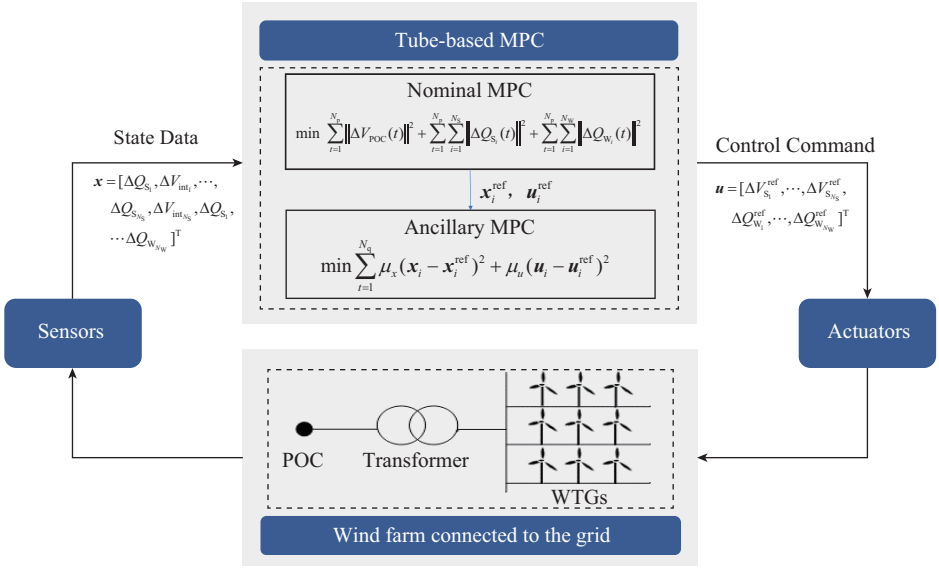

Fig. 3. Tube-based MPC control process considering malicious cyber-attack.

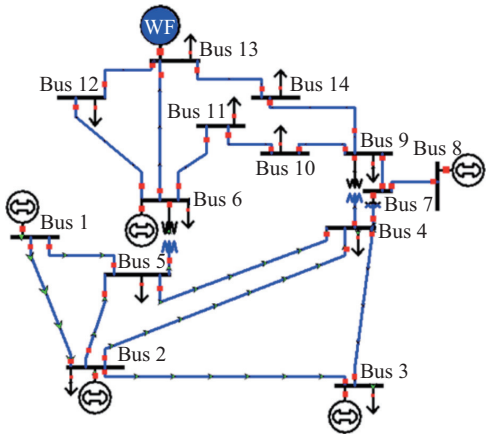

Fig. 4. Structure of the modified IEEE 14-bus test feeder.

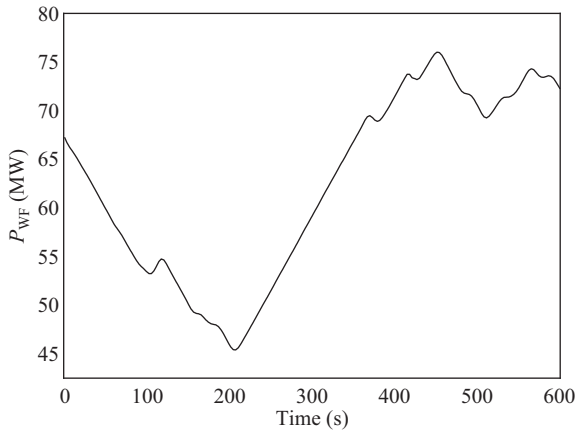

Fig. 5. Active power profile of the wind farm.

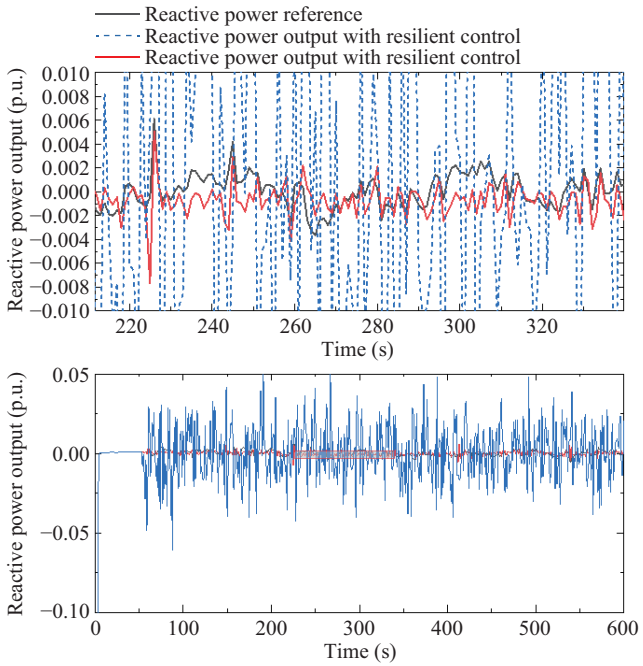

Fig. 6. Reactive power output of wind farms under random attacks on sensors on the modified IEEE 14-bus system.

power time profile with the TMPC algorithm is the same as that of the MPC algorithm, as shown in Fig. 6, certifying their identical performance on achieving optimality of the same objective without disturbances. After the attack occurs (50∼600 s), reactive power output without the TMPC control algorithm fluctuates violently and deviates greatly from the reference value, as shown in the blue solid line of Fig. 6. With the TMPC control, reactive power output can be regulated in the vicinity of the reference value, forming a 'tube' around the reference.

Figure 7 shows the time profile of V_{POC} with and without cyber-attacks on the modified IEEE 14-bus system. In 0∼50 s, both the MPC algorithm and TMPC algorithm can stabilize V_{POC} to the rated value (1.00 p.u.). In 50∼600 s, after the attack, voltage deviates greatly, and fluctuation range is large with conventional MPC algorithm. However, with the pro-

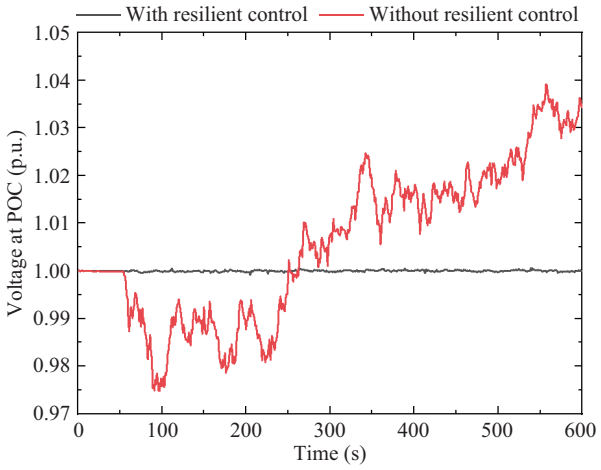

Fig. 7. Voltage at POC under random attacks on sensors on the modified IEEE 14-bus system.

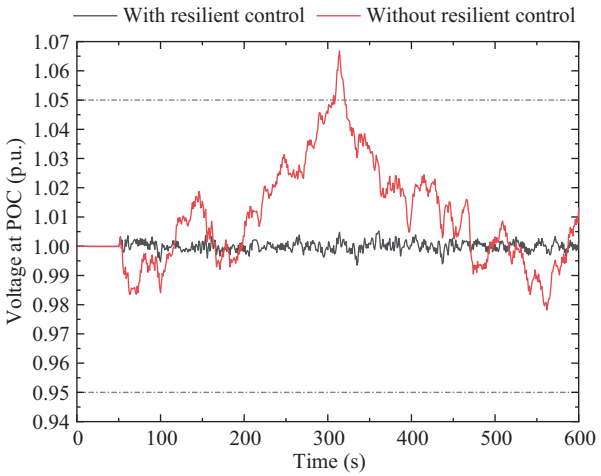

Fig. 8. Voltage at POC under random attacks on sensors on the modified IEEE 118-bus system.

posed TMPC algorithm, voltage fluctuates mildly around the rated value. The comparison of statistical indicators in these two cases can be summarized in Table I. Since standard deviation is a key indicator reflecting the volatility of data, it can be seen from the results in Table I that the TMPC algorithm plays an important role in voltage stability against cyber-attacks. The same conclusions are valid here as in the IEEE 118 bus network, as Fig. 8 shows. However, due to the different sizes of the simulation systems, its control speed is different. For each control period, the computation time of IEEE 118-bus system with the wind farm is about 0.4∼0.5 s (with Intel(R) Core (TM) I5-8250U CPU @ 1.60GHz 1.80GHz and MATLAB R2021a). Under the same configuration, the computation time of IEEE 14-bus system is about 0.08∼0.1 s.

B. Case 2: Actuator Attacks

The performance of the proposed strategy under actuator attacks is evaluated with $\dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u}^{\mathrm{a}}$, where $\boldsymbol{u}^{\mathrm{a}}$ is the control output under actuator attacks.

Figures 9, 10, and 11 show simulation results of conventional MPC and the proposed strategy under actuator attacks on a modified IEEE 14-bus system. It can be seen in Fig. 9 that, without the proposed strategy, there is a significant deviation between output and reference value when actuator attacks are initiated. By comparing reactive power output profiles with and without the TMPC algorithm, the case with the tube-based control scheme outperforms the conventional one with significantly less deviation from reference. Comparisons between the two cases can be summarized as shown in Table II. It can be seen from Table II that the induced deviation with the proposed strategy is much smaller than that of the conventional strategy.

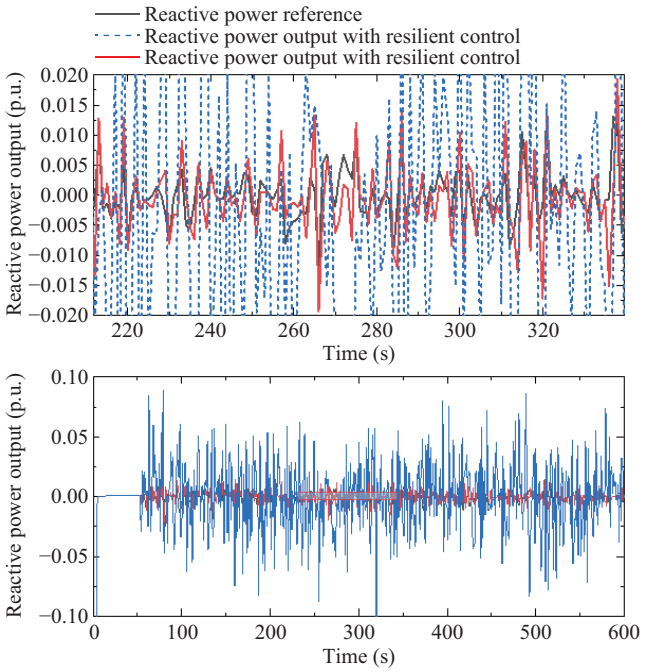

Fig. 9. Reactive power output of wind farms under random attacks on actuators on the modified IEEE 14-bus system.

As shown in Fig. 10, similar to the case of sensor attacks,

TABLE I
COMPARISON OF TWO CASES

Description		With the Proposed Strategy	Without the Proposed Strategy
Reactive Power Output	Maximum deviation from reference value	0.005 78	0.053 94
	Minimum deviation from reference value	−0.007 98	−0.062 14
	Average deviation from reference value	−0.000 23	0.000 42
	Standard Deviation	0.021 225	0.027 171
V_{POC}	Maximum deviation from reference value	0.000 58	0.039 15
	Minimum deviation from reference value	−0.000 82	−0.025 19
	Average deviation from reference value	−0.000 019	0.006 090
	Standard Deviation	0.000 160	0.016 205

TABLE II
COMPARISON OF TWO CASES

Description	Indicators	With the Proposed Strategy	Without the Proposed Strategy
Reactive Power Output	Maximum deviation from reference value	0.027 33	0.088 37
	Minimum deviation from reference value	−0.015 36	−0.123 36
	Average deviation from reference value	−0.000 01	−0.000 02
	Standard Deviation	0.022 049	0.036 458
V_{POC}	Maximum deviation from reference value	0.002 56	0.039 09
	Minimum deviation from reference value	−0.001 54	−0.034 61
	Average deviation from reference value	0.000 003	0.005 727
	Standard Deviation	0.000 479	0.018770

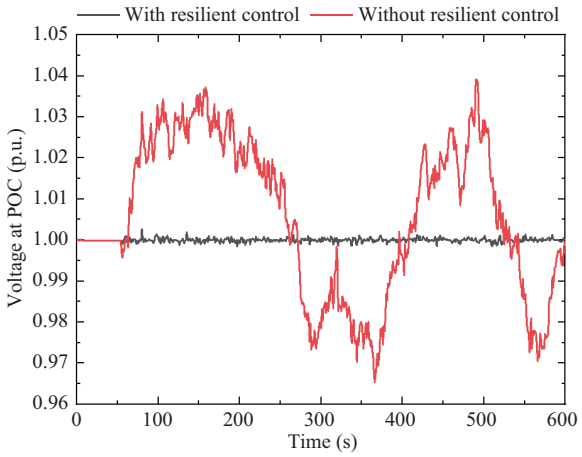

Fig. 10. Voltage at POC under random attacks on actuators on the modified IEEE 14-bus system.

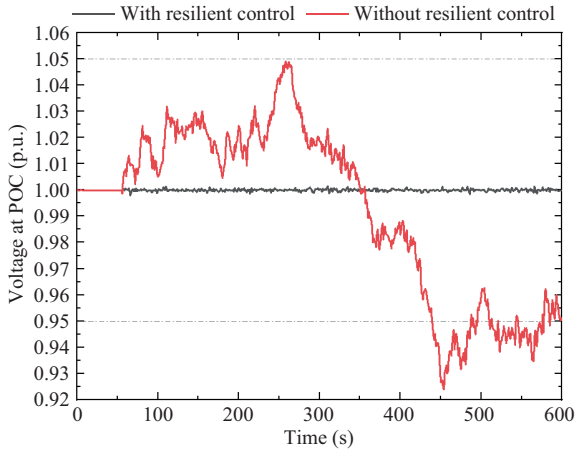

Fig. 11. Voltage at POC under random attacks on actuators on the modified IEEE 14-bus sy stem under the extreme circumstance.

V_{POC} fluctuates greatly when the attack occurs without the proposed strategy. When the TMPC algorithm is applied, voltage is stabilized near the rated value.

Figure 11 shows a more extreme case of V_{POC} under cyber-attacks. After the attack, V_{POC} exceeds the safe range (normally 0.95 p.u. $\sim$ 1.05 p.u., as shown by the dotted line in Fig. 11). However, with the proposed strategy, V_{POC} is always regulated near the vicinity of the rated value. Results confirm the effectiveness of the proposed strategy in sustaining optimal voltage control against cyber-attacks.

Similar to case 1, the same conclusions are valid here as in the IEEE 118 bus network, as Fig. 12 shows.

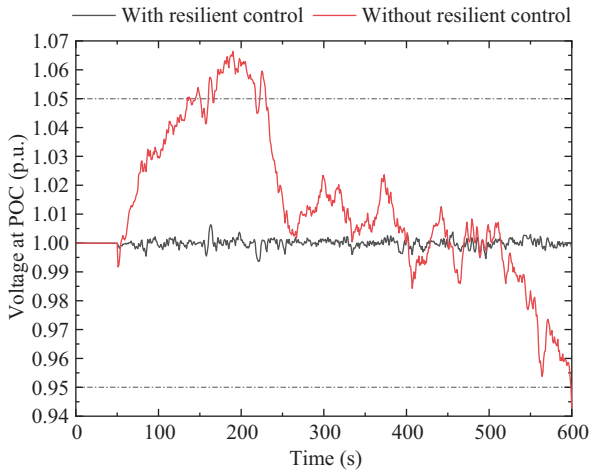

Fig. 12. Voltage at POC under random attacks on actuators on the modified IEEE 118-bus system.

VII. CONCLUSION

An attack-resilient optimal voltage control method is proposed to eliminate the influence of cyber-attacks on voltage optimized control in this paper. Based on the discrete-time control model of wind farms, the voltage-optimized control problem is formulated to minimize voltage deviation at the POC and achieve smooth regulation of wind turbines. The TMPC is then introduced to eliminate the detrimental effects of cyber-attacks on sensors and actuators. Simulation results of the modified IEEE 14-bus and 118-bus systems have demonstrated the proposed strategy can efficiently achieve almost the same voltage optimization and stability under cyber-attacks as those of ideal cases under no cyber-attacks. This proves the TMPC algorithm is an effective method for attack-resilient voltage-optimized control of wind farm-integrated power grids.

APPENDIX

The objective function shown as (10) can be rewritten as:

$$\boldsymbol{J} = \|\boldsymbol{C}\boldsymbol{D}\boldsymbol{x} + \boldsymbol{F}\|^2 + \boldsymbol{u}^2 \tag{A1}$$

where x and u are defined in (5)–(6), respectively. $\boldsymbol{C} = \left[\frac{\partial|V_{\mathrm{POC}}|}{\partial Q_{\mathrm{S}}}, 0, \frac{\partial|V_{\mathrm{POC}}|}{\partial Q_{\mathrm{W1}}}, \frac{\partial|V_{\mathrm{POC}}|}{\partial Q_{\mathrm{W2}}}, \cdots, \frac{\partial|V_{\mathrm{POC}}|}{\partial Q_{\mathrm{WN_W}}}\right]$, $\boldsymbol{D}$ is an identity matrix with $\boldsymbol{D}(2,2) = 0$, and $\boldsymbol{F} = V_{\mathrm{POC}} - V_{\mathrm{POC}}^{\mathrm{ref}}$.

Equation (A1) can be transformed into the following form with multiple iterations in a time period:

$$\bar{\boldsymbol{J}} = \boldsymbol{U}^{\mathrm{T}}(\bar{\boldsymbol{N}} + \boldsymbol{Q})\boldsymbol{U} + 2(\boldsymbol{M}\boldsymbol{x})^{\mathrm{T}}\boldsymbol{P}\boldsymbol{N}\boldsymbol{U} + \boldsymbol{x}^{\mathrm{T}}\bar{\boldsymbol{M}}\boldsymbol{x} \tag{A2}$$

where

$$\boldsymbol{M} = \boldsymbol{C}\boldsymbol{D}\bar{A},\ \boldsymbol{N} = \boldsymbol{C}\boldsymbol{D}\bar{B}$$
$$\bar{\boldsymbol{M}} = \boldsymbol{M}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{M},\ \bar{\boldsymbol{N}} = \boldsymbol{N}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{N}$$
$$\bar{\boldsymbol{A}} = \begin{bmatrix} \boldsymbol{A} & & & \\ & \boldsymbol{A}^2 & & \\ & & \ddots & \\ & & & \boldsymbol{A}^p \end{bmatrix}$$
$$\bar{\boldsymbol{B}} = \begin{bmatrix} \boldsymbol{B} & & & & \\ \boldsymbol{A}\boldsymbol{B} & \boldsymbol{B} & & & \\ \boldsymbol{A}^2\boldsymbol{B} & \boldsymbol{A}\boldsymbol{B}^2 & \boldsymbol{B} & & \\ \vdots & \vdots & \vdots & & \\ \boldsymbol{A}^{p-1}\boldsymbol{B} & \boldsymbol{A}^{p-2}\boldsymbol{B}^2 & \cdots & \boldsymbol{A}\boldsymbol{B}^{p-1} & \boldsymbol{B} \end{bmatrix}$$

and $\boldsymbol{U} = [u_1, u_2, \cdots u_{\mathrm{p}}]^{\mathrm{T}}$. p is the iteration times in a time period. P and Q are identity matrices.

Suppose the optimized control variables with and without attacks are $\boldsymbol{U}^*$ and $\boldsymbol{U}^{\mathrm{a}*}$. Since $\bar{\boldsymbol{J}}$ is a convex function, we have

$$\boldsymbol{U}^{\mathrm{T}}\tilde{\boldsymbol{N}}\boldsymbol{U} + 2\boldsymbol{x}^{\mathrm{T}}\tilde{\boldsymbol{M}}\boldsymbol{U} \geq \boldsymbol{U}^{*\mathrm{T}}\tilde{\boldsymbol{N}}\boldsymbol{U}^* + 2\boldsymbol{x}^{\mathrm{T}}\tilde{\boldsymbol{M}}\boldsymbol{U}^* \quad \text{(A3)}$$

where $\tilde{\boldsymbol{N}} = \bar{\boldsymbol{N}} + \boldsymbol{Q}$ and $\tilde{\boldsymbol{M}} = \boldsymbol{M}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{N}$.

If there were no deviation between voltage optimization results with and without cyber-attacks, (A3) would be $\boldsymbol{U}^{\mathrm{T}}\tilde{\boldsymbol{N}}\boldsymbol{U} + 2\boldsymbol{x}^{\mathrm{T}}\tilde{\boldsymbol{M}}\boldsymbol{U} \geq \boldsymbol{U}^{\mathrm{a}*\mathrm{T}}\tilde{\boldsymbol{N}}\boldsymbol{U}^{\mathrm{a}*} + 2\boldsymbol{x}^{\mathrm{T}}\tilde{\boldsymbol{M}}\boldsymbol{U}^{\mathrm{a}*}$, that is,

$$\begin{aligned} &\boldsymbol{U}^{\mathrm{T}}\tilde{\boldsymbol{N}}\boldsymbol{U} + 2\boldsymbol{x}^{\mathrm{a}\mathrm{T}}\tilde{\boldsymbol{M}}\boldsymbol{U} - 2a\tilde{\boldsymbol{M}}\boldsymbol{U} \\ &\geq \boldsymbol{U}^{\mathrm{a}*\mathrm{T}}\tilde{\boldsymbol{N}}\boldsymbol{U}^{\mathrm{a}*} + 2\boldsymbol{x}^{\mathrm{a}\mathrm{T}}\tilde{\boldsymbol{M}}\boldsymbol{U}^{\mathrm{a}*} - 2a\tilde{\boldsymbol{M}}\boldsymbol{U}^{\mathrm{a}*} \end{aligned} \quad \text{(A4)}$$

Since $U^{\mathrm{a}*}$ is the optimal solution of the objective function (4) with cyber-attacks, we have

$$\boldsymbol{U}^{\mathrm{T}}\tilde{\boldsymbol{N}}\boldsymbol{U} + 2\boldsymbol{x}^{\mathrm{a}\mathrm{T}}\tilde{\boldsymbol{M}}\boldsymbol{U} \geq \boldsymbol{U}^{\mathrm{a}*\mathrm{T}}\tilde{\boldsymbol{N}}\boldsymbol{U}^{\mathrm{a}*} + 2\boldsymbol{x}^{\mathrm{a}\mathrm{T}}\tilde{\boldsymbol{M}}\boldsymbol{U}^{\mathrm{a}*} \quad \text{(A5)}$$

where $\tilde{M}$ can be rewritten as

$$\tilde{\boldsymbol{M}} = \begin{bmatrix} \boldsymbol{A}^2\sum\left(\frac{\partial|V_{\mathrm{POC}}|}{\partial Q_{\mathrm{S}}}\right) & & & \\ & 0 & & \\ & & \boldsymbol{A}^2\sum\left(\frac{\partial|V_{\mathrm{POC}}|}{\partial Q_{\mathrm{W}}}\right) & \\ & & & \ddots \\ & & & \boldsymbol{A}^2\sum\left(\frac{\partial|V_{\mathrm{POC}}|}{\partial Q_{\mathrm{W}}}\right) \end{bmatrix}$$

So $\tilde{\boldsymbol{M}}$ is a semi-definite matrix.

Obviously, there is a $\boldsymbol{U}$ that makes $2a\tilde{\boldsymbol{M}}\boldsymbol{U}^{\mathrm{a}*} - 2a\tilde{\boldsymbol{M}}\boldsymbol{U} < 0$, which contradicts the assumption of (A4). Therefore, the initial assumption of "there was no deviation between voltage optimization results with and without cyber-attacks, $\boldsymbol{U}^* = \boldsymbol{U}^{\mathrm{a}*}$" must be false.

Analysis when actuator attack occurs is similar to the sensor attack.

So, cyber-attacks will bias voltage optimization results.

REFERENCES

[1] K. G. Boroojeni, M. H. Amini, and S. S. Iyengar, *Smart Grids: Security and Privacy Issues*. Cham: Springer, 2017.

[2] S. J. Xin, Q. L. Guo, H. B. Sun, B. M. Zhang, J. H. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2375–2385, Sep. 2015.

[3] K. Wu, J. Li, Y. Zhu, S. Miao, S. Zhu and C. Zhou, "Interactive visual analysis on the attack and defense drill of grid cyber-physical systems," *CSEE Journal of Power and Energy Systems*, vol. 7, no. 1, pp. 45–56, Jan. 2021.

[4] B. Ti, J. Wang, G. Li and M. Zhou, "Operational Risk-averse Routing Optimization for Cyber-physical Power Systems," *CSEE Journal of Power and Energy Systems*, vol. 8, no. 3, pp. 801–811, May 2022.

[5] W. Qiu, C. Li, Q. Tang, K. Sun, Y. Liu and W. Yao, "Attack Detection for Spoofed Synchrophasor Measurements Using Segmentation Network," *CSEE Journal of Power and Energy Systems*, vol. 8, no. 5, pp. 1327–1337, Sep. 2022.

[6] L. Xu, Q. L. Guo, Y. J. Sheng, S. M. Muyeen, and H. B. Sun, "On the resilience of modern power systems: a comprehensive review from the cyber-physical perspective," *Renewable and Sustainable Energy Reviews*, vol. 152, pp. 111642, Dec. 2021.

[7] Defense Use Case, "Analysis of the cyber attack on the Ukrainian power grid," Electricity Information Sharing and Analysis Center (E-ISAC), Washington, 2016.

[8] J. Devanny, L. R. F. Goldoni, and B. P. Medeiros, "The 2019 Venezuelan blackout and the consequences of cyber uncertainty," *Revista Brasileira de Estudos de Defesa*, vol. 7, no. 2, pp. 37–57, Jul. 2021.

[9] Y. F. Wang, K. L. Gao, T. Zhao, and J. Qiu, "Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph," *Proceedings of the CSEE*, vol. 36, no. 6, pp. 1490–1499, Mar. 2016.

[10] L. Langer, P. Smith, M. Hutle, and A. Schaeffer-Filho, "Analysing cyber-physical attacks to a smart grid: a voltage control use case," in *Proceedings of 2016 Power Systems Computation Conference (PSCC)*, 2016, pp. 1–7.

[11] M. Moness and A. M. Moustafa, "A survey of cyber-physical advances and challenges of wind energy conversion systems: prospects for internet of energy," *IEEE Internet of Things Journal*, vol. 3, no. 2, pp. 134–145, Apr. 2016.

[12] V. K. Singh, R. Sharma, and M. Govindarasu, "Testbed-based performance evaluation of attack resilient control for wind farm SCADA system," in *Proceedings of 2020 IEEE Power & Energy Society General Meeting (PESGM)*, 2020, pp. 1–5.

[13] S. Y. Zhao, Q. M. Yang, P. Cheng, R. L. Deng, and J. H. Xia, "Adaptive resilient control for variable-speed wind turbines against false data injection attacks," *IEEE Transactions on Sustainable Energy*, vol. 13, no. 2, pp. 971–985, Apr. 2022.

[14] L. Xu, Q. L. Guo, Z. G. Wang, and H. B. Sun, "Modeling of time-delayed distributed cyber-physical power systems for small-signal stability analysis," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3425–3437, Jul. 2021.

[15] Y. Chen, S. W. Huang, F. Liu, Z. S. Wang, and X. W. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019.

[16] R. Fu, Y. Xu, Y. Tang, and Q. Wang, "Petri net-based voltage control strategy under false data injection attack," *Transactions of the Institute of Measurement and Control*, vol. 42, no. 14, pp. 2622–2631, Jun. 2020.

[17] C. Cameron, C. Patsios, P. C. Taylor, and Z. Pourmirza, "Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3010–3019, May 2019.

[18] M. A. Rahman, M. S. Rana, and H. R. Pota, "Mitigation of frequency and voltage disruptions in smart grid during cyber-attack," *Journal of Control, Automation and Electrical Systems*, vol. 31, no. 2, pp. 412–421, Feb. 2020.

[19] A. Gusrialdi, Y. Xu, Z. H. Qu, and M. A. Simaan, "Resilient cooperative voltage control for distribution network with high penetration distributed energy resources," in *Proceedings of the 18th European Control Conference*, 2020, pp. 1533–1539.

[20] M. S. Sadabadi, S. Sahoo, and F. Blaabjerg, "Stability-oriented design of cyberattack-resilient controllers for cooperative DC Microgrids," *IEEE Transactions on Power Electronics*, vol. 37, no. 2, pp. 1310–1321, 2022.
[21] Y. L. Chen, D. L. Qi, H. N. Dong, C. Y. Li, Z. M. Li, and J. L. Zhang, "A FDI attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1929–1938, May 2021.
[22] S. M. Sotoudeh and B. HomChaudhuri, "A robust MPC-based hierarchical control strategy for energy management of hybrid electric vehicles in presence of uncertainty," in *Proceedings of 2020 American Control Conference (ACC)*, 2020, pp. 3065–3070.
[23] P. Kou, D. L. Liang, R. Gao, Y. B. Liu, and L. Gao, "Decentralized model predictive control of hybrid distribution transformers for voltage regulation in active distribution networks," *IEEE Transactions on Sustainable Energy*, vol. 11, no. 4, pp. 2189–2200, Oct. 2020.
[24] A. Oshnoei, M. Kheradmandi, S. M. Muyeen, and N. D. Hatziargyriou, "Disturbance observer and tube-based model predictive controlled electric vehicles for frequency regulation of an isolated power grid," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4351–4362, Sep. 2021.
[25] P. Xie, Y. W. Jia, H. K. Chen, J. Wu, and Z. X. Cai, "Mixed-stage energy management for decentralized microgrid cluster based on enhanced tube model predictive control," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 3780–3792, Sep. 2021.
[26] C. Lyu, Y. W. Jia, and Z. Xu, "Real-time operation optimization of microgrids with battery energy storage system: a tube-based model predictive control approach," arXiv: 2104.04819, 2021.
[27] J. Wei, Y. J. Cao, Q. W. Wu, C. B. Li, S. Huang, B. Zhou, and D. Xu, "Coordinated droop control and adaptive model predictive control for enhancing HVRT and post-event recovery of large-scale wind farm," *IEEE Transactions on Sustainable Energy*, vol. 12, no. 3, pp. 1549–1560, Jul. 2021.
[28] S. Huang, Q. W. Wu, J. Zhao, and W. Liao, "Distributed optimal voltage control for VSC-HVDC connected large-scale wind farm cluster based on analytical target cascading method," *IEEE Transactions on Sustainable Energy*, vol. 11, no. 4, pp. 2152–2161, Oct. 2020.
[29] S. Huang, Q. W. Wu, Y. F. Guo, and F. Rong, "Hierarchical active power control of DFIG-based wind farm with distributed energy storage systems based on ADMM," *IEEE Transactions on Sustainable Energy*, vol. 11, no. 3, pp. 1528–1538, Jul. 2020.
[30] H. R. Zhao, Q. W. Wu, Q. L. Guo, H. B. Sun, S. J. Huang, and Y. S. Xue, "Coordinated voltage control of a wind farm based on model predictive control," *IEEE Transactions on Sustainable Energy*, vol. 7, no. 4, pp. 1440–1451, Oct. 2016.
[31] K. Christakou, J. Y. Leboudec, M. Paolone, and D. C. Tomozei, "Efficient computation of sensitivity coefficients of node voltages and line currents in unbalanced radial electrical distribution networks," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 741–750, Jun. 2013.
[32] R. Tóth, *Modeling and Identification of Linear Parameter-Varying Systems*, Berlin: Springer, 2010.
[33] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach*. Springer Science & Business Media, 2012.
[34] X. Liu, Z. Y. Li, X. D. Liu, and Z. Y. Li, "Masking transmission line outages via false data injection attacks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1592–1602, Jul. 2016.
[35] W. Langson, I. Chryssochoos, S. V. Raković, and D. Q. Mayne, "Robust model predictive control using tubes," *Automatica*, vol. 40, no. 1, pp. 125–133, Jan. 2004.
[36] I. Kiaei and S. Lotfifard, "Tube-based model predictive control of energy storage systems for enhancing transient stability of power systems," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6438–6447, Nov. 2018.

Zhenming Li received her B.E.E degree at Zhejiang University, Hangzhou, China, in 2017. She is currently pursuing a Ph.D. degree from the College of Electrical Engineering, Zhejiang University, Hangzhou, China. Her current research interests include voltage optimization and control of renewable energy and cyber-physical security with application in smart grids.

Minghao Wang received the B.Eng.(Hons.) degree in Electrical and Electronic Engineering from Huazhong University of Science and Technology, Wuhan, China, and the University of Birmingham, U.K. in 2012, and the M.Sc. and the Ph.D. degree, both in Electrical and Electronic Engineering, from The University of Hong Kong, Hong Kong, China, in 2013 and 2017, respectively. Currently, he is a Research Assistant Professor in the Department of Electrical Engineering, the Hong Kong Polytechnic University. His search interests include power systems and power electronics.

Yunfeng Yan is currently a postdoc in Zhejiang University, Hangzhou, China. She received the Ph.D. degree in Electrical Engineering in December 2019. Her research interests include computer vision and machine learning systems, and distributed estimation and control of networked systems.

Donglian Qi received her Ph.D. degree in Control Theory and Control Engineering from Zhejiang University, Hangzhou, China, in March 2002. Since then, she has been with the College of Electrical Engineering, Zhejiang University where she is currently a professor. Her current research interests include the basic theory and application of cyber physical power system (CPPS), digital image processing, artificial intelligence, and electric operation and maintenance robots.

Zhao Xu received the B.Eng., M.Eng., and Ph.D. degrees from Zhejiang University, Hangzhou, China, in 1996, National University of Singapore, Singapore, in 2002, and The University of Queensland, Brisbane, QLD, Australia, in 2006, respectively. He is currently a Professor with the Department of Electrical Engineering, Hong Kong Polytechnic University, Hong Kong. He was with the Center for Electric Power and Energy, Technical University of Denmark. His research interests include demand side, grid integration of renewable energies and EVs, electricity market planning and management, and AI applications in power engineering.

Jianliang Zhang received his Ph.D. degree in Control Theory and Control Engineering from Zhejiang University, Hangzhou, China, in June 2014. Since then, he has been working with the College of Electrical Engineering, Zhejiang University (ZJU). He was a visiting scholar at Hongkong Polytechnic University (PolyU) (2016-2017). His current research interests include distributed optimization, with applications to energy/power systems, and cyber-physical security with applications in smart grids.

Zezhou Wang graduated from Zhejiang University with a master's degree in Electrical Engineering, and now works in Haiyan power supply company of State Grid Zhejiang Electric Power Co., Ltd.