Electrical Power and Energy Systems 137 (2022) 107713

Contents lists available at ScienceDirect

International Journal of Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

A modified model predictive control method for frequency regulation of microgrids under status feedback attacks and time-delay attacks

Zhengrong Chen, Zhaoxi Liu, Lingfeng Wang *

Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, United States

ARTICLE INFO

Keywords:
Microgrid
Secondary frequency regulation
Cybersecurity
Model predictive control
Time-delay estimation

ABSTRACT

As a promising technology to integrate renewable energy and enable decentralized energy management, microgrid (MG) offers an appealing network architecture due to its potential economic, environmental, and technical benefits. However, with the increasing deployment of intelligent devices and the growing network interconnectivity, communication channels and controllers for MGs become more vulnerable to emerging cyber threats. Two types of attacks are considered in this paper, including the data integrity attacks on the system status feedback and time-delay attacks which may disrupt the control of the MGs and lead to adverse consequences. A modified model predictive control (MPC) scheme is proposed for the secondary frequency control of MGs based on the online status switching method and generalized cross correlation (GCC) estimation to detect the real system status and time delay injected to the control system. The Euclidean metric is used in the online status switching method to obtain the real system states. Meanwhile, the GCC based delay estimation is developed to detect and track the time delay posed by attacks in the real-time operation. Case studies under different scenarios of the attacks are conducted, and the simulation results verify the effectiveness of the proposed MPC scheme under the cyberattacks.

1. Introduction

Renewable energy sources (RESs) are appealing alternatives to the conventional fossil-fuel based generation units in the modern power systems to provide power supply and reduce the carbon emissions. However, the integration of RESs would introduce additional disturbances and uncertainties to the power systems. Significant efforts will be required to keep the secure and stable operation of the grid. Microgrid (MG) is regarded as a promising architecture in the power systems due to its potential economic, environmental and technical benefits [1]. It consists of distributed generation (DG) units, (e.g., diesel engines, micro turbines, combined heat and power (CHP) units and especially RESs such as PV and wind turbines), energy storage systems (ESS) and loads [2,3].

MGs can be operated in both grid-connected and islanded modes [4]. In the grid-connected mode, active and reactive power can be supplied by or exported to the main grid through the point of common coupling (PCC). However, in the islanded mode, the MG is disconnected from the main grid, and the control becomes more difficult and complicated without the support of the main grid. More advanced control algorithms are required in the islanded mode to achieve proper frequency regulations, which are critical to maintaining the stability of MGs.

Generally, the hierarchical control structure of MGs consists of three levels, namely the primary, secondary, and tertiary control [5–7]. Droop control, as a predominant mechanism, is commonly used to accomplish the active power sharing in the primary control. However, in the steady state, the system will reach a new operating point where frequency deviations may be introduced as a result of the droop control method, which needs to be eliminated by the secondary control. Due to the complexity of the frequency regulation problems in the modern MG systems and uncertainty caused by RES, traditional PID controllers may be unable to provide a satisfactory performance. Several works have been done to handle the frequency regulation problems by proposing improved control strategies. Ref. [8] presents a secondary control method with no communications for islanded MGs, where a switch control between two configurations according to a time-dependent protocol is used to achieve frequency restoration. Event-trigger based secondary control methods are proposed in [9] to reduce the communication band-width. In [10], a new online intelligent approach using a combination of the fuzzy logic and PSO technique for optimal tuning of the PI frequency controllers is proposed. Compared with the existing control strategies, MPC methods [11–13] are promising to address the uncertainties and disturbances, which have been widely used in the frequency regulation fields. Meanwhile, MPC is robust in

* Corresponding author.
E-mail address: l.f.wang@ieee.org (L. Wang).

https://doi.org/10.1016/j.ijepes.2021.107713
Received 18 May 2021; Received in revised form 2 October 2021; Accepted 15 October 2021
Available online 15 November 2021

Nomenclature

Abbreviations

BESS	Battery energy storage system
CHP	Combined heat and power
DEG	Diesel engine generator
DG	Distributed generation
DoS	Denial-of-service
ESS	Energy storage systems
FC	Fuel cell
FDI	False data injection
FESS	Flywheel energy storage system
GCC	Generalized cross correlation
LSTM	Long short term memory
LTI	Linear time invariant
MG	Microgrid
ML	Machine learning
MPC	Model predictive control
PCC	Point of common coupling
PI	Proportional–Integral
PID	Proportional–Integral–Derivative
PV	Photovoltaics
RESs	Renewable energy sources
SISO	Single Input Single Output
TDC	Time Delay Control
WTG	Wind turbine generator

Parameters

λ_1, λ_2	Weighting factors of MPC
τ_{max}	Boundary of time-delay variable
D, M	System inertia constant/damping constant
K_{BESS}, K_{FESS}	Gain factors of BESS/FESS
K_{DEG}	Gain factor of DEG
K_{FC}	Gain factor of FC
K_{PV}	Gain factor of PV
K_{WTG}	Gain factor of WTG
N_1, N_2	The boundaries of the costing horizon of MPC
N_u	Control horizon of MPC
R	Coefficient of droop control of DEG
T_s	Sampling time
$T_{BESS}, T_{FESS}, T_{WTG}, T_{PV}, T_{FC}$	Time constants of BESS/FESS/WTG/PV/FC
T_{IN}, T_C, T_g, T_t	Time constants of inverter/converter/generator/governor
$u_{min,1}, u_{max,1}$	Boundary of control variable Δu_1
$u_{min,2}, u_{max,2}$	Boundary of control variable Δu_2

Variables

$\Delta\Phi, \Delta f$	Deviation of solar radiance/System frequency deviation
ΔP_e	Difference between the power demand and the total power generation
ΔP_{DEG}	Power deviation of DEG
ΔP_{FC}	Power deviation of FC
$\Delta P_{FESS}, \Delta P_{BESS}$	Power deviation of FESS/BESS
ΔP_{Load}	System overall load disturbance
ΔP_{PV}	Power deviation of PV
$\Delta P_W, \Delta P_{WTG}$	Output mechanical power/real power deviation of WTG
$\Delta u_1, \Delta u_2$	Control signal of DEG/FC
τ	Time delay variable
S_{BESS}, S_{FESS}	Status of the BESS/FESS
x_{mpc}	New state variables of modified MPC

real-time operation and can consider system dynamics and communication delays as well [14,15]. However, communication delays are different from time-delay attacks since time-delay attacks can also be implemented in other parts of the MGs. Moreover, few of them consider the compromised MG system due to cyberattacks on the controller or communication infrastructure.

The modern power grids rely on the open communication infrastructure to improve the efficiency of the operations, which makes them vulnerable to the cyberattacks implemented by adversaries. In general, an intruder attempts to get into the IT infrastructure of the control systems and eventually disrupt the control of the components in the power grid [16]. For example, in 2015, the Ukrainian power grid was attacked by malicious cyber-attackers, which was considered the first cyberattack event causing power blackouts [17]. In 2018, the Los Angeles Department of Water and Power was hacked in just a few hours. Colonial pipeline as the critical energy supply had been down in 2020 due to cyberattack and burglars installed malicious computers onto a grid providing power to a chunk of the Northwest in Oregon, 2021. The typical cyberattack methods include the false data injection (FDI) attacks [18,19], denial-of-service (DoS) attacks [20,21] and time-delay attacks [22,23]. The FDI attacks and time-delay attacks are two important types of cyberattacks which could be fatal to the power systems, which are in the scope of this paper. The FDI attacks exploit the sensory measurements and inject false information in the control system, which would eventually degrade or totally damage the control performance. To improve the cybersecurity of power system, several studies have formulated effective mitigation methods. A general dynamic security assessment method based on Ensemble Decision Trees (EDT) is proposed in [24] to assess and predict the security states of the grid. A series of attack models and scenarios on networked control systems are analyzed and simulated in [25]. In [26], an observer based detector using the tie-line power estimation is proposed to exclude the FDI signal from the control loop and an H infinity controller is used to mitigate the influence from FDI attacks. The authors of [27] develop a model-based anomaly detection and attack mitigation algorithm on AGC schemes. However, many of the FDI attack defend techniques do not consider time-delay attack of the communication channel [28,29]. The time-delay attacks attempt to delay various signals in the control system to make system unstable, e.g., deployed in the sensing loop. For detection and mitigation of the time-delay attack, a ML-based safety classifier is presented and a two-tier mitigation method to tune the control gain is develop in [30]. Another learning-based LSTM approach is designed to estimate the delay values [31] and a three-stage defend strategy based on dynamic game theory is applied to mitigate time delay attack [32]. However, most of attack estimation methods, which have considerable computational requirement, are computational expensive and complex for real-time operation. To the best of our knowledge, the existing studies have not investigated the intelligent and resilient control strategies for the MG frequency control considering multiple potential cyberattacks in the same framework. Time delay control (TDC) has been successfully applied in the linear time invariant (LTI) systems and single input single output (SISO) systems to estimate the unknown dynamics by time delay variables [33,34]. However, the drawback of the existing TDC methods lies in the

difficulty of tuning a proper error feedback gain. Meanwhile, the time-varying time delay and multiple attack scenarios are not considered in these models. It is true that the time-delay attack can be mitigated to some extent by optimizing the prediction horizon when it is large enough. However, it does not make sense to extend the prediction horizon without limit which may sacrifice the control performance. Tuning the parameters of the controller is another major issue which is difficult to be realized online. Moreover, due to the dynamic change of the MG model under multiple attacks, the system frequency cannot be kept stable only by optimizing the prediction horizon. Therefore, the Generalized cross correlation (GCC) time-delay estimation based method is proposed in this paper, with which constant and time-varying time delay can be detected and the estimated states can be updated online to adaptively regulate the MG system frequency control under the attacks.

Motivated by [10] and [35], this paper focuses on the secondary frequency control of the islanded AC MGs considering potential cyber-attacks. A MPC-based control framework is developed for the secondary frequency control of MGs. Two specific types of attacks are considered under our framework. First, an FDI attack may be posed by adversaries to compromise the data integrity of the system status feedback to the controller, which is termed as status feedback attack in this study. Meanwhile, a time-delay attack can be applied on the measurements in the frequency control system. Then a modified MPC scheme is built for the secondary frequency control of MGs considering both types of cyberattacks. Several case studies were performed to verify the effectiveness of the proposed MPC scheme.

The main contributions of this paper are summarized as follows:

1. Frequency regulation of an isolated AC MG including WTG, DEG, PV panel and energy storage systems is studied in this work, where a centralized MPC framework is designed to prevent MG from collapsing during dramatic change in load demand or the large-scale integration of RESs. Meanwhile, status feedback attacks and time-delay attacks are defined in the attack scheme to compromise the frequency controller.
2. Based on the MPC framework, an effective attack mitigation methodology which only requires information exchange among neighboring units and is able to achieve a satisfactory computational efficiency is proposed. To mitigate the status feedback attacks, a Euclidean metric based online status switching method is proposed to detect the real system statuses, and update the state vector in the controller to obtain desirable control performance with the proposed MPC scheme. Moreover, an online time-delay estimation method based on the GCC algorithm is devised to detect time delay injected by the attacks.
3. Considering the implementation of both status feedback attacks and time-delay attacks in the system, a modified MPC algorithm is proposed that combines the online status switching method and the online time-delay estimation method to ensure the stability, reliability and cybersecurity of MGs.

The rest of the paper is organized as follows. An islanded MG with the time-delay attacks and status feedback attacks is modeled in Section 2. In Section 3, a modified MPC scheme based on the online status switching method and GCC estimation is developed to mitigate the cyberattacks. The case studies of the proposed MPC scheme are presented and discussed in Section 4, followed by the conclusions in Section 5 and future work in Section 6.

2. Modeling of AC MG frequency control with time delay attacks and status feedback attacks

2.1. Configuration of islanded AC MG

The MG is equipped with ESS and DGs including RES to supply the connected loads. Based on the model of the isolated MG system in [10], the configuration of the MG is shown in Fig. 1. The MG contains the conventional DEG, PV panel, WTG, fuel cell (FC) system, battery energy storage system (BESS), and flywheel energy storage system (FESS). Power electronic interfaces are used for the synchronization of AC sources including the WTG and the connection of DC sources including the PV panel, FC, and energy storage devices to the MG. Both the FC and DEG are considered as parts of the secondary frequency control to mitigate the frequency deviation.

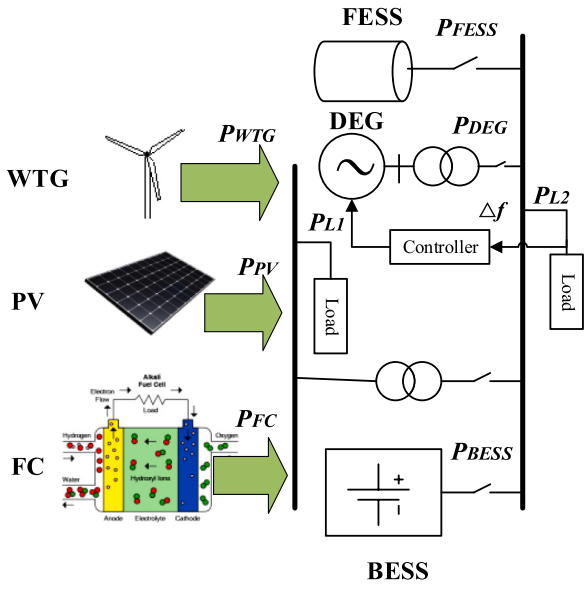

Fig. 1. Configuration of Islanded AC MGs.

2.2. Power balance function and transfer functions

$$P_{Load} = P_{L1} + P_{L2} = P_{WTG} + P_{PV} + P_{FC} + P_{DEG} \pm P_{FESS} \pm P_{BESS} \quad (1)$$

where the power exchange between the ESS and the MG can be bidirectional. The FC and DEG deliver power to the MG system when the generation from the WTG and PV is insufficient. High-order mathematical models including the non-linearity and controllers should be employed to formulate the dynamic behaviors of practical WTG, PV, DEG, FC, BESS, FESS, etc. more precisely. For large-scale power system simulations, however, simplified transfer functions are generally adopted for the computational efficiency with acceptable accuracy. Therefore, the power losses are not considered in this paper. A three-order model of the FC is used for frequency studies [36]. The transfer functions of the WTG, PV, FC, DEG and ESS are, respectively, represented by a first-order lag [37] as follows:

$$G_{WTG}(s) = \frac{K_{WTG}}{1 + sT_{WTG}} = \frac{\Delta P_{WTG}}{\Delta P_W} \quad (2)$$

$$G_{PV}(s) = \frac{K_{PV}}{1 + sT_{PV}} = \frac{\Delta P_{PV}}{\Delta \phi} \quad (3)$$

$$G_{FC}(s) = \frac{K_{FC}}{1 + sT_{FC}} \cdot \frac{1}{1 + sT_{IN}} \cdot \frac{1}{1 + sT_C} = \frac{\Delta P_{FC}}{\Delta f} \quad (4)$$

$$G_{DEG}(s) = \frac{K_{DEG}}{1 + sT_g} \cdot \frac{1}{1 + sT_t} = \frac{\Delta P_{DEG}}{\Delta f} \quad (5)$$

$$G_{BESS}(s) = \frac{K_{BESS}}{1 + sT_{BESS}} = \frac{\Delta P_{BESS}}{\Delta f} \quad (6)$$

$$G_{FESS}(s) = \frac{K_{FESS}}{1 + sT_{FESS}} = \frac{\Delta P_{FESS}}{\Delta f} \quad (7)$$

In the autonomous MG system, the total power generation must meet the total power demand of the connected loads to maintain the

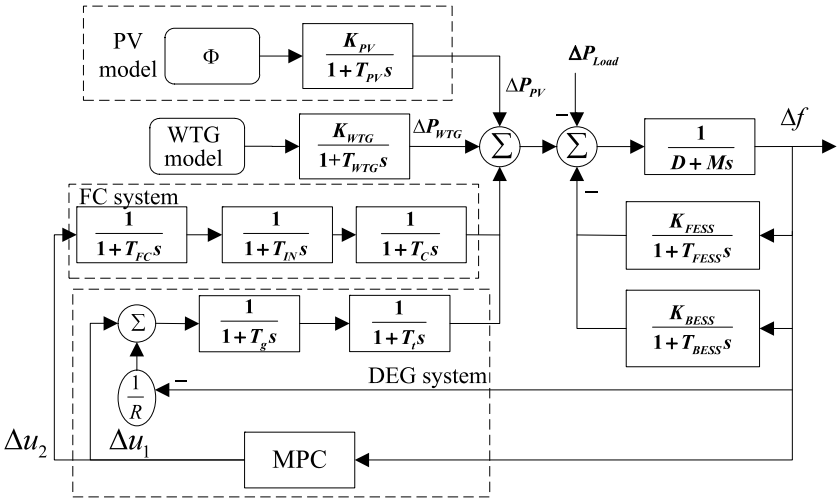

Fig. 2. MPC framework for secondary frequency control of MGs.

stable operations. However, due to the difference between the power demand reference P_d^* and the total power generation P_g, which is denoted by ΔP_e, the system frequency would deviate from the reference. Hence, the P-f control method is applied in the primary control to track the reference frequency.

$$\Delta P_e = P_d^* - P_g \tag{8}$$

The system frequency variation is calculated by

$$\Delta f = \frac{\Delta P_e}{K_{sys}} \tag{9}$$

where K_{sys} is the system frequency characteristic constant of the MG. The transfer function for the system frequency variation to per unit power deviation can be expressed by

$$G_{sys}(s) = \frac{\Delta f}{\Delta P_e} = \frac{1}{K_{sys}(1+sT_{sys})} = \frac{1}{D+sM} \tag{10}$$

where D and M are, respectively, the equivalent inertia constant and damping constant [38].

2.3. Model predictive control strategy

The MPC technique has been widely used in various control issues of power system due to its salient characteristics [39–42]. It is able to handle control constraints in a systematic way, feature a high performance for nonlinear systems, and allow for optimized control decisions in a rolling horizon fashion. In this study, an MPC controller is developed for the secondary frequency control of MGs. The MPC framework for the MG frequency control is shown in Fig. 2. Both the FC system and the DEG system are controllable units to adapt to the fluctuation of load disturbance and renewable energy generation to maintain the stability of the system frequency. For example, if the output power of PV and WTG increase, the system operator can decrease the generation from DEG and/or FC (depending on the control strategy) to keep the balance of the system and regulate the system frequency. However, their models are different from each other. Two individual control variables are obtained as the outputs of the MPC controller. Meanwhile, the BESS and FESS can participate in the frequency regulation and enable the balance between load and generation in the grid. They may work at the same time, or only one of them are connected, or both of them are disconnected, depending on the system reconfiguration. Thus, the system frequency is influenced by the operations of the FC and DEG systems, and the FESS/BESS. Thus, they are included in the system model of the MPC framework. However, it should be noted that, the BESS and FESS are not assumed to be directly controlled and regulated by the secondary frequency control commends from the system operator in the considered MG system. They are assumed to participate and support the system frequency control with a negative response to the system frequency deviation through their local controllers when they are connected to the MG, as shown in Fig. 2. The goal of the MPC frequency control is to minimize the frequency deviation Δf, which should be equal to zero. Δu_1, Δu_2 are the control signals to the DEG and FC units for their generation adjustments respectively. The dynamic of output power of WTG and PV is considered, which along with load disturbance are considered stochastic disturbances to the system. Similar to the dynamic MG model in [43,44], a linear stochastic state space function of the proposed MG system can be expressed based on the former transfer functions as follows:

$$\begin{cases} \dot{x} = Ax + Bu + F(\Delta P_{load} + \Delta P_{WTG} + \Delta P_{PV}) \\ y = Cx \end{cases} \tag{11}$$

$$x = \begin{bmatrix} \Delta f & \Delta P_{DEG} & \Delta \dot{P}_{DEG} & \Delta P_{FC} & \Delta \dot{P}_{FC} & \Delta \ddot{P}_{FC} & \Delta P_{FESS} & \Delta P_{BESS} \end{bmatrix}^{\mathrm{T}} \tag{12}$$

$$y = \Delta f \tag{13}$$

$$u = \begin{bmatrix} \Delta u_1 & \Delta u_2 \end{bmatrix}^{\mathrm{T}} \tag{14}$$

$$A = \begin{bmatrix} -\frac{D}{M} & \frac{1}{M} & 0 & \frac{1}{M} & 0 & 0 & \frac{1}{M} & \frac{1}{M} \\ 0 & -\frac{1}{T_t} & \frac{1}{T_t} & 0 & 0 & 0 & 0 & 0 \\ -\frac{1}{RT_g} & 0 & -\frac{1}{T_g} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{T_c} & \frac{1}{T_c} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{T_{IN}} & \frac{1}{T_{IN}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{1}{T_{FC}} & 0 & 0 \\ \frac{1}{T_{FESS}} & 0 & 0 & 0 & 0 & 0 & -\frac{1}{T_{FESS}} & 0 \\ \frac{1}{T_{BESS}} & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{T_{BESS}} \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 & \frac{1}{T_g} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{T_{FC}} & 0 & 0 \end{bmatrix}^{\mathrm{T}}$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$F = \begin{bmatrix} -\frac{1}{M} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{\mathrm{T}} \tag{15}$$

Since the MPC controller is realized with digital devices, the discrete state-space model is derived from the continuous model in Eq. (11)

Table 1
Statuses of FESS and BESS.

	S_{FESS}	S_{BESS}
Situation 1	0	0
Situation 2	1	0
Situation 3	0	1
Situation 4	1	1

based on the sampling time T_s, which can be presented as:

$$\begin{cases} x(k+1) = A_d x(k) + B_d u(k) + F_d(\Delta P_{load}(k) + \Delta P_{WTG}(k) + \Delta P_{PV}(k)) \\ y(k) = C_d x(k) \end{cases} \tag{16}$$

where $A_d = e^{AT_s}$; $B_d = (A_d - I)A^{-1}B$, which is valid under the assumption A is invertible; $F_d = F$; $C_d = C$.

$$x(k) = [\Delta f(k) \quad \Delta P_{DEG}(k) \quad \Delta \dot{P}_{DEG}(k) \quad \Delta P_{FC}(k) \quad \Delta \dot{P}_{FC}(k) \quad \Delta \ddot{P}_{FC}(k) \quad \Delta P_{FESS}(k) \quad \Delta P_{BESS}(k)]^{\mathrm{T}} \tag{17}$$

2.4. Status feedback attacks

The ESS units are important components in the MG. As shown in Eq. (11) and Fig. 2, the outputs of the ESS are responsive to the system frequency deviation. Thus, the statuses of the ESS units are essential to the frequency control. Two binary variables, denoted by S_{FESS} and S_{BESS}, are used to indicate the statuses of the FESS and BESS. If $S_{FESS/BESS} = 0$, the BESS/FESS is assumed to be disconnected from the MG. Otherwise, the BESS/FESS is assumed to be connected to the MG and responsive to the frequency deviation. According to the combination of the two variables, there are in total 4 situations as listed in Table 1.

The system model based on accurate status feedback of the system components is essential for the MPC controller to determine the optimized control signals. If the status feedback of the BESS and/or FESS are contaminated by adversaries, it may degrade the performance of the frequency control and compromise the system stability. For example, when only BESS is available, $S_{FESS} = 0$ and $S_{BESS} = 1$. However, the feedback signals can be maliciously altered if a status feedback attack is successfully implemented. The controller would receive the false information such as $S_{FESS} = 1$, $S_{BESS} = 1$ showing that both ESS are still connected to the MG and responsive to the frequency deviation. This will lead to an inaccurate system model, invalid control strategies and consequently degraded performance of the frequency control. The diagram of the MPC based control system under the status feedback attack is depicted in Fig. 3.

From Fig. 3, we can see that the hacker may attack the MPC by injecting false data into the feedback signals of the ESS statuses. The system state vector in Eq. (17) can be revised as follows:

$$\tilde{x}(k) = \begin{bmatrix} x_1(k) \\ \vdots \\ S_{FESS} \cdot x_7(k) \\ S_{BESS} \cdot x_8(k) \end{bmatrix} \tag{18}$$

Further detection and online switching from different conditions are required to address the status feedback attacks so that the accurate system model can be obtained, based on which the optimized strategies for the frequency control of MG can be achieved.

2.5. Time-delay attacks

Usually, the local information measured by sensors is sent to the frequency controller and control center through the communication channel. Then the controller estimates the current system states which are essential for the control decision making. After the control signals are determined according to the current system states, the frequency controller sends the control signals to the local generation units, e.g., DEG and FC, through the communication channel. Due to the high dependence on the communication, the system would be vulnerable to time-delay attacks in which the attacker delays the measurements sent to the controller. An illustration of the load frequency control system under the time-delay attacks is depicted in Fig. 4.

In the time-delay attacks, the attacker injects a time delay in the measurement from the sensor to the controller. The diagram of the MPC based frequency control system considering the time-delay attack in the control loop is shown in Fig. 5. The state space function of the system can be expressed similarly as Eq. (11). However, an exponential block $e^{-s\tau}$ is added, where τ is the time delay of the measurement due to the attack. With the time-delay attack, the control signal is modified as

$$U = -K\hat{X} \tag{19}$$

and the new state after attack can be modeled by

$$\hat{X} = \begin{bmatrix} \hat{x_1} \\ \hat{x_2} \\ \vdots \\ \hat{x_8} \end{bmatrix} = \begin{bmatrix} x_1(t-\tau) \\ x_2(t-\tau) \\ \vdots \\ x_8(t-\tau) \end{bmatrix} \tag{20}$$

For the discrete-time model, the state variables can be rewritten as:

$$\hat{X} = \begin{bmatrix} \hat{x_1(k)} \\ \hat{x_2(k)} \\ \vdots \\ \hat{x_8(k)} \end{bmatrix} = \begin{bmatrix} x_1(k-\tau/T_s) \\ x_2(k-\tau/T_s) \\ \vdots \\ x_8(k-\tau/T_s) \end{bmatrix} \tag{21}$$

Since a time-delay attack could sabotage the performance of the frequency control, the proper strategies should be developed to detect the delay attacks and stipulate a response plan.

3. Attack mitigation methodology

3.1. Online switching method

Due to the different statuses of the BESS and FESS, the state space functions that describe the dynamic model of the MG system vary from one to the other. Only with the accuracy state space functions, the output of the system can be predicted properly by the MPC, and the deviation of frequency can be regulated accurately. As the historical data of the MPC control signal output u is known, the predicted frequency deviation from the former situations can be obtained. The Euclidean metric is proposed to measure the difference between the current system frequency deviation and the predicted frequency deviation. By comparing the Euclidean metric of the deviation between the current data and the predicted data with different statuses of the ESS, the actual statuses of the BESS and FESS can be recognized with the lowest error. The mechanism of the proposed status feedback online detection is shown in Fig. 6.

According to the state space function of each situation shown by the status blocks in Fig. 6, $\Delta f_1, \Delta f_2, \Delta f_3, \Delta f_4$ can be calculated respectively during the specific observation time.

$$r_i = \mathrm{RMSE} = \sqrt{\frac{\sum_{k=1}^{n}(\Delta f_1 - \Delta f)^2}{n}} \tag{22}$$

Then the RMSE (Root Mean Squared Error) is utilized to measure the error between $\Delta f_1, \Delta f_2, \Delta f_3, \Delta f_4$ and Δf. The situation with the least RMSE is considered as the real situation and the corresponding status feedback of the BESS and FESS will be updated. Then, the MPC controller is modified by the updated status feedback in real time. In the immediate control step, the predicted states and control signals are

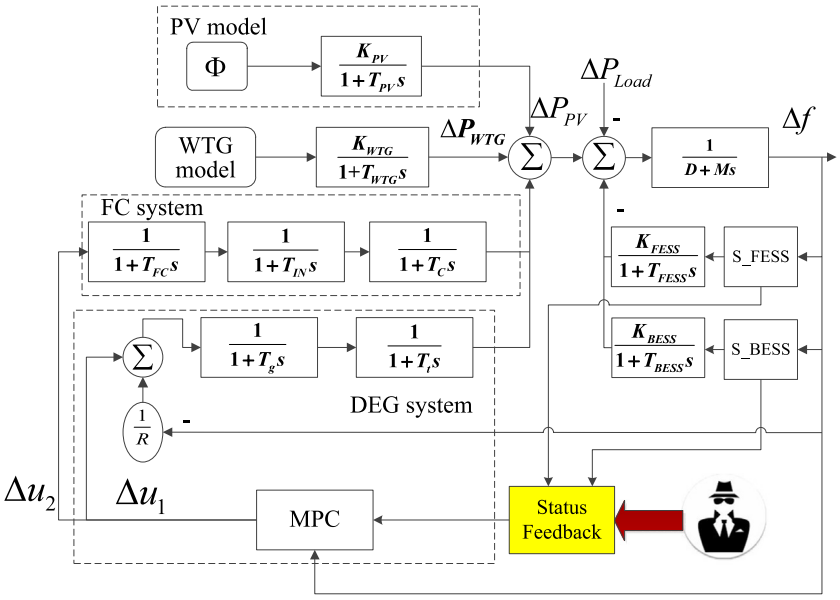

Fig. 3. Model of status feedback attacks.

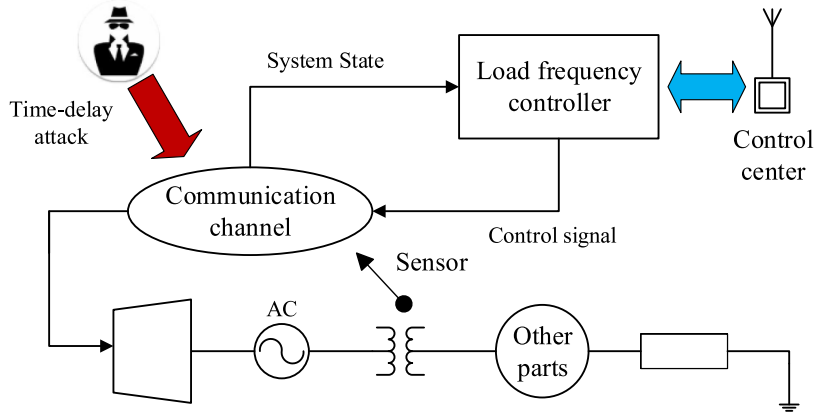

Fig. 4. Load frequency control system under time-delay attacks.

computed by the MPC with the updated state space function of the actual model according to statuses of BESS and FESS.

3.2. Online time-delay estimation technique

To mitigate the time-delay attack, a new control scheme is proposed which involves the use of the plant model, a time-delay estimator, and the MPC controller to control system frequency. The control scheme will detect and track the time delays introduced by adversaries and guide the plant to track the reference to guarantee the system stability. Fig. 7 shows the diagram of the proposed control method.

This paper proposes a GCC based time-delay estimator to update the delay estimation. Then the state space will be modified with the estimated time-delay. According to the updated plant model, the MPC controller adjusts the control signals to eliminate the fluctuation caused by delay of the measurement. For simplification, the system being dealt with can be approximated in the plant block to describe the dynamic system.

In general, the time delay τ is an unknown variable. It should be noted that $x(t-\tau)$ is sent to the controller from the sensor. Thus, at every instance of time, variables $u(t)$, A, B and $x(t-\tau)$ are known to the controller. In contrast, the current $x(t)$ and the time delay are unknown. It is essential to estimate τ firstly and then $x(t)$ correctly. Through the plant model, we can calculate the estimated state value $\hat{x}(t)$ since $A, B, F, \Delta P_{load}, \Delta P_{WTG}, \Delta P_{PV}$ are known and $u(t)$ processed by the MPC controller in the preceding intervals are saved. Then, a GCC estimator is used to estimate the time delay τ by comparing $\hat{x}(t)$ and $x(t-\tau)$.

The GCC algorithm is widely used in the field of signal processing to analyze the time gap between two signals [45,46]. In the discrete time model, $\hat{x}(t)$ and $x(t-\tau)$ can be reformulated with sampling time T_s by array elements $y_1(n)$ and $y_2(n)$ respectively:

$$y_1(n) = [\hat{x}(0), \hat{x}(1), \ldots, \hat{x}(k), \ldots, \hat{x}(m)] = s(n) + O(n)$$

$$y_2(n) = [\bar{x}(0), \bar{x}(1), \ldots, \bar{x}(k), \ldots, \bar{x}(m)] = \alpha s(n+D) \quad (23)$$

where $s_1(n)$ is the real signal obtained from the sensor, $O(n)$ is the noise signal. Signal $s_1(n)$ is assumed to be uncorrelated with $O(n)$. $\bar{x}(k) = x(k-\tau/T_s)$, if $k < \tau/T_s$, $\bar{x}(k) = 0$. For convenience, it is assumed that $\alpha = 1$. Here, the cross-correlation function is proposed to determine

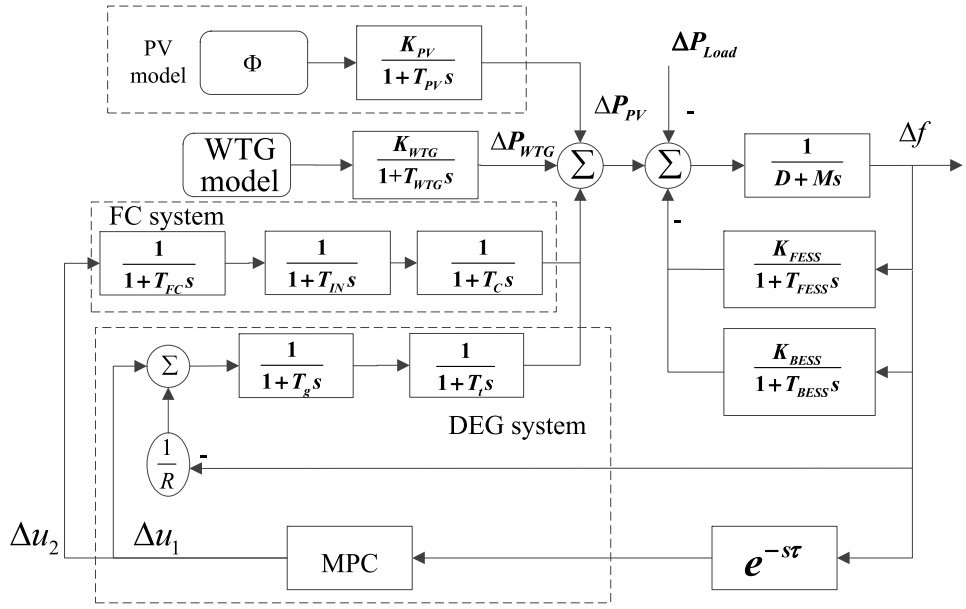

Fig. 5. Dynamic model of MPC frequency control with time-delay attacks.

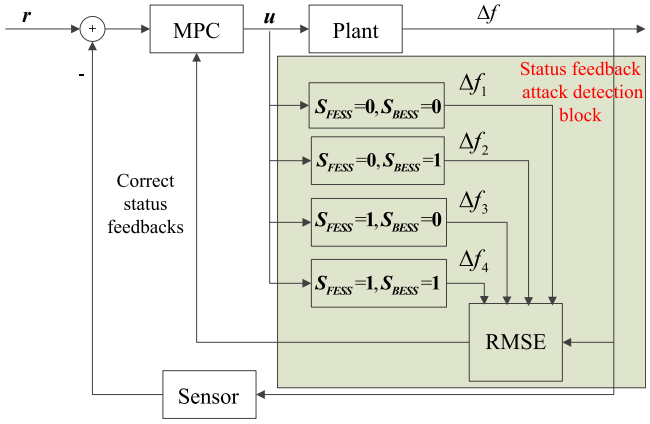

Fig. 6. Status feedback attack online detection block.

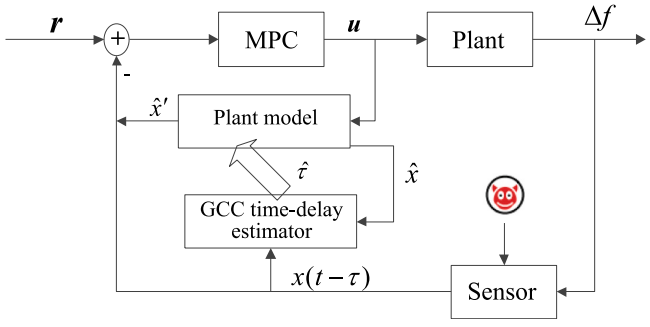

Fig. 7. Status feedback attack online detection block.

the time delay by

$$R_{y_1y_2}(\bar{\tau}) = E\{y_1(n)y_2(n-\bar{\tau})\} = E\{s(n+D-\bar{\tau})s(n)\} = R_s(D-\bar{\tau}) \tag{24}$$

where $R_s(D-\bar{\tau})$ represents the autocorrelation of $s(n)$. The peak of the cross-correlation function provides an estimate of the delay. The GCC algorithm aims to improve the accuracy of the delay estimate $\hat{D}$ where $y_1(n)$ and $y_2(n)$ are filtered. Therefore, the generalized cross-correlation

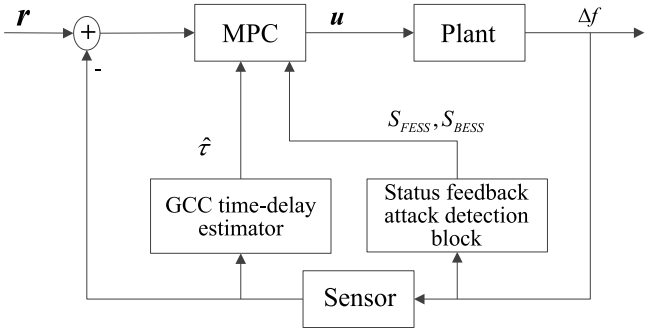

Fig. 8. Modified MPC scheme for the frequency control of MG under the attacks.

function based on the phase transform (PHAT) is expressed as follows:

$$R^{(g)}_{y_1y_2}(\bar{\tau}) = F^{-1}\left[P_{y_1y_2(\omega)}W(\omega)\right] = R_{y_1y_2}(\bar{\tau}) * \omega(\bar{\tau}), \quad W(\omega) = \frac{1}{\left|P_{y_1y_2}(\omega)\right|} \tag{25}$$

Then, the time delay estimation $\hat{D}$ can be calculated by:

$$\hat{D} = \arg\max_{D}(R^{(g)}_{y_1y_2}(\bar{\tau})) \tag{26}$$

3.3. Modified MPC algorithm

Based on the analysis in the previous subsections, a modified MPC scheme is proposed for the frequency control of MG under the attacks, which is shown in Fig. 8. The state-space model is same as Eq. (16), however, the new state estimation is:

$$x_{mpc} = \begin{bmatrix} x_1(k-\tau/T_S) \\ \vdots \\ x_6(k-\tau/T_S) \\ S_{FESS}\cdot x_7(k-\tau/T_S) \\ S_{BESS}\cdot x_8(k-\tau/T_S) \end{bmatrix} \tag{27}$$

The cost function of the MPC is defined as:

$$J(N_1, N_2, N_u) = \sum_{j=N_1}^{N_2} [\Delta f(k+j|k)]^2 + \lambda_1 \sum_{j=0}^{N_u} [\Delta u_1(k+j-1)]^2 + \lambda_2 \sum_{j=0}^{N_u} [\Delta u_2(k+j-1)]^2 \quad (28)$$

$$s.t.$$

$$u_{min,1} \le \Delta u_1 \le u_{max,1}$$

$$u_{min,2} \le \Delta u_2 \le u_{max,2}$$

The first term of the cost function minimizes the frequency deviation Δf-error between the prediction of the system frequency and its set-point, and the second and third terms minimize the control efforts, where λ_1, λ_2 are weighting factors. N_1, N_2 are the boundaries of the costing horizon, and N_u is the control horizon.

The detailed steps of implementation are as follows:

Step 1: Initialize time-delay estimate $\hat{\tau}$, plant model state estimate $\hat{x}$, reference signal r and MPC controller state x_{mpc}.

Step 2: Obtain the plant state measurement (i.e., the sensed output states of the plant $x(k-\tau/T_s)$), which could be hacked by attackers.

Step 3: Compute the current state estimate $\hat{x}(k)$ according to the plant state space model. The discrete equation can be approximated as follows:

$$\dot{\hat{x}}(k+1) = A\hat{x}(k) + Bu(k) + F(\Delta P_{load}(k) + \Delta P_{WTG}(k) + \Delta P_{PV}(k)) \quad (29)$$

Step 4: Use the GCC algorithm to compute the time-delay estimate $\hat{\tau}$ by comparing $\hat{x}(k)$ and $x(k-\tau/T_s)$. In order to reduce the computational complexity, an observation interval T is adopted to compute the cross-correlation function.

Step 5: Compute the state estimation $x_i(k)$, which will be stored as historical data to compute the RMSE, for the 4 situations of different statuses of BESS and FESS by using $\hat{\tau}$ and $u(k)$. Then calculate r_i based on Eq. (22) when comparing $\Delta f_1, \Delta f_2, \Delta f_3, \Delta f_4$ with Δf. Then the actual statuses of the BESS and FESS are obtained from the situation with the least error.

Step 6: Modify the MPC controller state model with the time-delay estimate $\hat{\tau}$ obtained in Step 3 and statuses of the FESS and BESS ($S_{FESS/BESS}$) obtained in Step 5, and then compute the new MPC controller state x_{mpc}.

Step 7: Compute the control signal $u(k)$ in the MPC controller. As the new MPC controller state x_{mpc} and the input of the modified MPC controller $e(k) = r(k) - x(k-\tau/T_s)$ are known, u can be set by the MPC optimization.

Step 8: To prevent runaway and dead-zone situations, bound the time-delay estimate by τ_{max} and the control signal by u_{min}, u_{max}.

Step 9: Repeat Steps 2–8.

4. Case studies

In order to illustrate the performance of the proposed MPC scheme for the frequency control of MG under attacks, case studies were conducted. Three scenarios based on different kinds of attacks were tested: (1) the scenario with status feedback attacks, (2) the scenario with time-delay attacks, and (3) the scenario with both status feedback attacks and delay attacks. In addition, both constant and time-varying delay attacks were analyzed in the case studies. For comparison, Case 1 to Case 3 do not consider the dynamic of PV and WTG, while they are simulated in Case 4 and Case 5.

4.1. Parameters

Nominal values of the DG and ESS units and loads are given in Table 2, and parameter values of the MG system are listed in Table 3. The MPC parameters are set to $T_s = 0.01$, $N_1 = 1$, $N_2 = 30$, $N_u = 5$, $\lambda_1 = \lambda_2 = 1$.

Table 2
Rated power of DG units and loads.

Rated power (kW)		Load (kW)	
WTG	100		
PV panel	30	P_{L1}	210
FC	70		
DEG	160		
FESS	45	P_{L2}	210
BESS	45		

Table 3
Parameter values of the block diagram.

Parameter	Value	Parameter	Value
D	0.015	T_g	0.08
M	0.1667	T_t	0.4
T_{FESS}	0.1	T_C	0.004
T_{BESS}	0.1	T_{IN}	0.04
T_{FC}	0.26	R	3
K_{PV}	1	T_{PV}	1.8
K_{WTG}	1	T_{WTG}	1.5
K_{BESS}	1	K_{FESS}	1

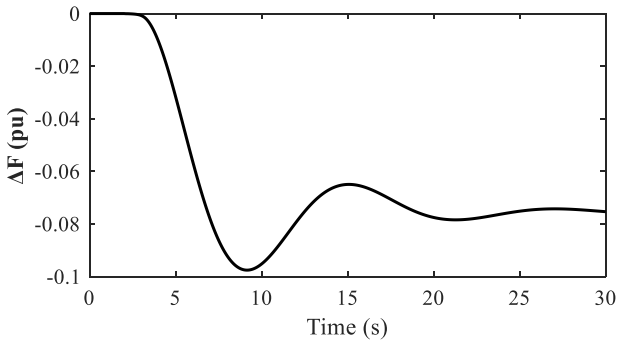

Fig. 9. Traditional MPC under status feedback attacks without mitigation.

4.2. Scenario 1: with status feedback attacks

Case 1: In this case, the FESS and BESS are assumed to be in the connected mode ($S_{FESS} = 1, S_{BESS} = 1$) which means they both participate the system frequency control. However, the state information is altered as $S_{FESS} = 0, S_{BESS} = 0$. As the MPC controller receives the false status feedback, the corresponding control signals would seriously deviate from the optimized values with the generic MPC approach.

The frequency response of case with traditional MPC under a load disturbance of 0.1 p.u. at $t = 2$ s is depicted in Fig. 9. It is shown that the status feedback attack causes the system instability when there are no mitigation measures. The system frequency completely loses track of the reference, presenting a divergent boundary.

In contrast, the results of the system frequency response with the proposed modified MPC scheme and the online detection of the statuses of BESS and FESS are shown in Fig. 10(a) and (b), respectively. Fig. 10(c) and (d) depict the power deviation of BESS/FESS. With the proposed MPC scheme, the system frequency returns to the reference promptly to keep the system stability after the load disturbance under the status feedback attack. When $t = 2.03$ s, the proposed Euclidean metric based algorithm detects the accurate status feedback of the ESS, where $S_{FESS} = 1, S_{BESS} = 1$. Therefore, the modified MPC controller can be adjusted to the actual states of the ESS and achieve the optimized control decisions.

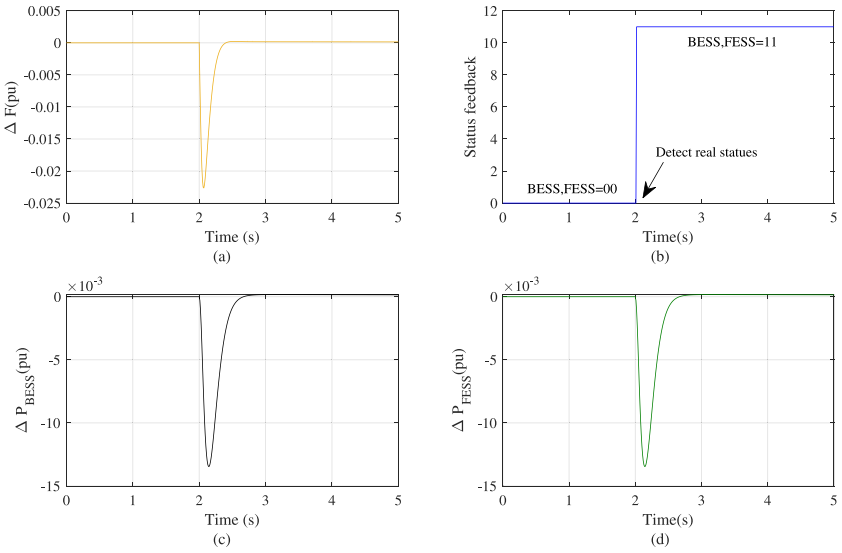

Fig. 10. The performance result in Case 1. (a) Frequency response. (b) Online detection of statuses of BESS and FESS. (c) The output power of BESS. (c) The output power of FESS.

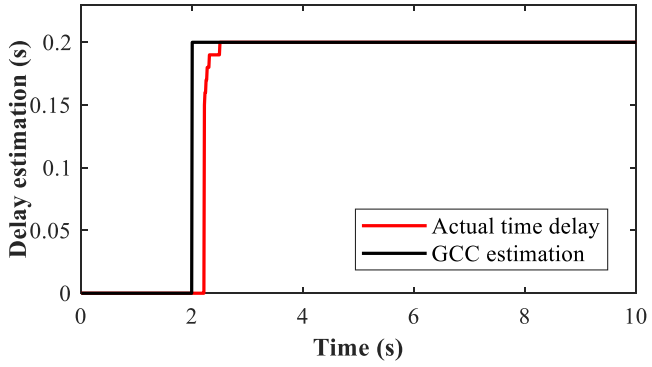

Fig. 11. GCC based delay estimation in Case 2.

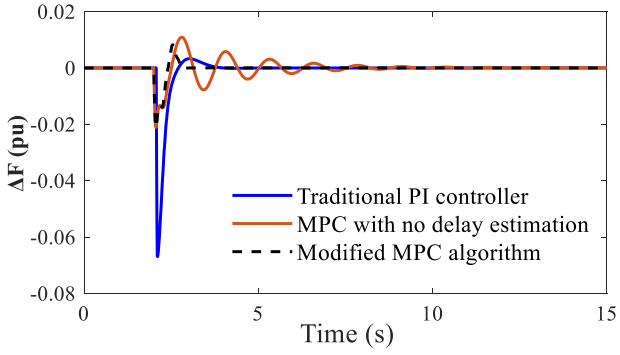

Fig. 12. Frequency response under time-delay attack in Case 2.

4.3. Scenario 2: with time delay attacks

Case 2: attacks with constant time-delay

In this case, the load increases by 0.1 p.u. at $t = 2$ s, and a constant 0.2 s time-delay is applied on the measurement to the MPC controller. With the proposed modified MPC method, the online delay estimation and the system frequency control performance are shown in Figs. 11 and 12, respectively.

From Fig. 11, it is shown that the proposed GCC based estimation method can detect and track the time-delay attack in a short time.

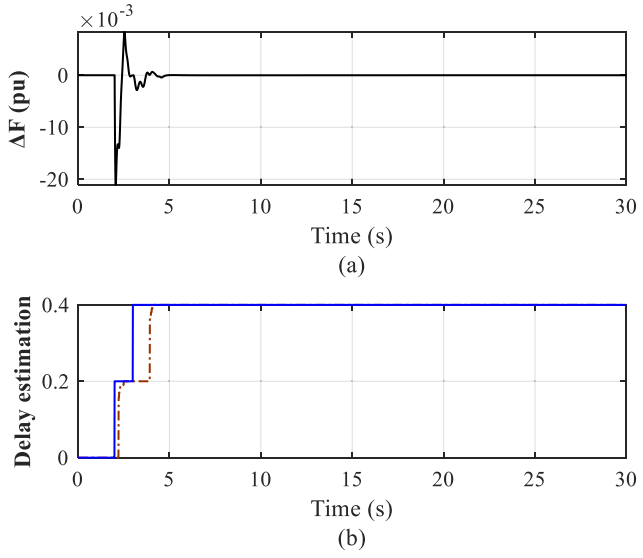

Fig. 13. (a) Frequency deviation in Case 3. (b) Time-delay estimation in Case 3.

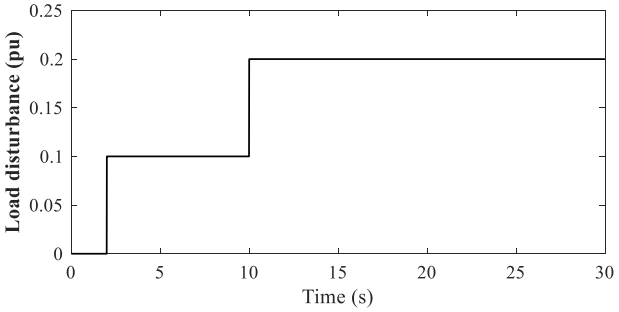

Fig. 14. Two steps load disturbance.

After obtaining the accurate delay, the system states in the modified MPC are adjusted immediately. It can be observed in Fig. 12 that the modified MPC algorithm based on the GCC estimation can make system frequency stable with less than 1.6 s adjustment time and 0.02 p.u.

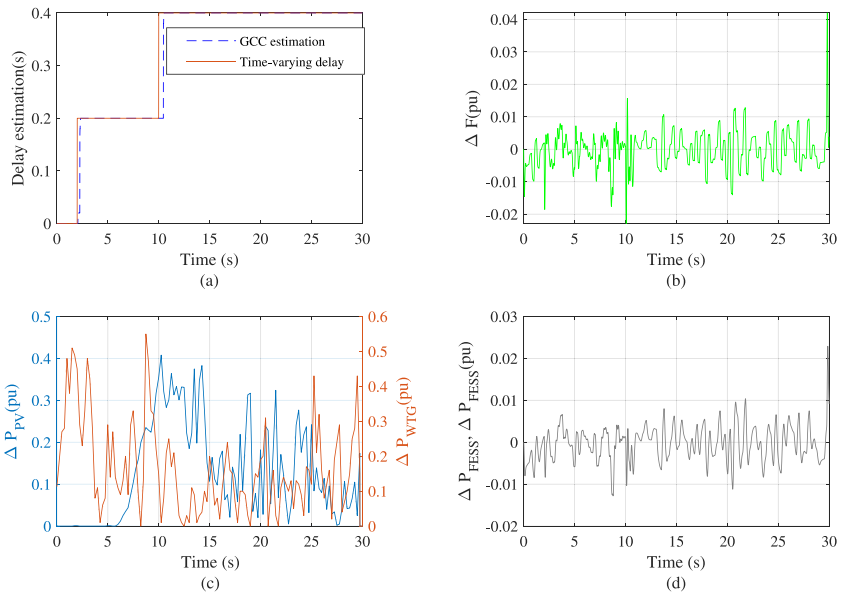

Fig. 15. The performance result in Case 4. (a) GCC time delay estimation. (b) Frequency response. (c) The PV and WTG output power. (d) The output power of BESS/FESS.

overshoot. The proposed MPC scheme significantly outperforms the PI controller and the traditional MPC without the attack mitigation method, which needs about 8 s to restore the frequency stability.

Case 3: attacks with time-varying delay

In this case, a time delay of 0.2 s is injected from $t = 2$ s to $t = 3$ s and it changes to 0.4 s after $t = 3$ s. Fig. 13 shows the system frequency and the result of the time-delay estimation. In the simulation, the load power increases by 0.1 p.u. since $t = 2$ s, causing a frequency drop at first. However, the proposed MPC scheme based on the GCC estimation can obtain satisfactory performance under the time-varying delay. Although the injected delay changes during the transient process, the system frequency is able to remain stable after t = 5 s and the overshoot is only about 0.02 p.u.

Case 4: two-step load disturbance

In this case, a two-step load disturbance is assumed whose value is 0.1 p.u. from $t = 2$ s to $t = 10$ s and 0.2. p.u. after $t = 10$ s, as shown in Fig. 14. Meanwhile, the time delay imposed by the attack is 0.2 s from $t = 2$ s to $t = 10$ s and it changes to 0.4 s after $t = 10$ s. Fig. 15(a) and (b) show the time-delay estimation and the frequency response of the MG system, respectively. The PV and WTG output power are given in Fig. 15(c). The output power of BESS/FESS is presented in Fig. 15(d). It can be seen that the GCC method estimates the time-delay due to the attack correctly and promptly. In other words, a longer delay results in more severe conditions for the frequency stability. The results verify the effectiveness of the modified MPC scheme under time-varying delay attacks and show dynamic performance considering the power deviation of PV and WTG.

4.4. Scenario 3: with both time delay attacks and status feedback attacks

Case 5: The implementation of status feedback attack is same as Case 1. Meanwhile, a 0.2 s time delay is applied on the system measurement and load disturbance of 0.1 p.u. is assumed since $t = 2$ s. The case results are shown in Fig. 16.

As expected, the GCC method detects and estimates the accurate time-delay rapidly within 0.4 s as indicated in Fig. 16(c). Meanwhile, with the proposed online switching method, the real status feedback of the ESS is obtained and updates in 0.02 s as shown in Fig. 16(b). As a result, the frequency response of the system under both types of attacks simultaneously are satisfying with the proposed MPC scheme. Seen in Fig. 16(d), the fluctuation of system frequency is within 0.05 p.u. boundary, which is reasonable and robust considering the dynamic of PV and WTG in the system.

From the results of Case 1 and Case 2 in the case studies, it can be concluded that the traditional MPC cannot address either the status feedback attack or the time-delay attack on the secondary frequency control of the MG. The simulation results verify the effectiveness of the proposed MPC scheme with online status switching method and GCC time-delay estimation in mitigating the impact of the status feedback attack or the time-delay attack. The proposed MPC based method can effectively mitigate the system frequency deviation under different scenarios of status feedback attacks and the time-delay attacks while the traditional MPC fails the task.

5. Conclusions

In this paper, a modified MPC scheme based on an online-switching method and GCC delay estimation is proposed for the secondary frequency control of MGs under status feedback attacks and time-delay attacks. As the status information of the BESS and FESS in the MG may be altered maliciously due to the status feedback attacks, an online switching method based on RMSE is proposed to identify the real statuses of the BESS and FESS. In the time-delay attacks, a delay can be injected in the system measurement to the controller. A GCC algorithm-based method is developed to estimate the time delay. With the modified system model considering the status feedback attacks and time-delay attacks, a new MPC scheme is built based on the online switching method and GCC-based estimation. Case studies with three scenarios under different types of attacks are conducted. The simulation results verify the effectiveness of the proposed method. The real statuses of the BESS/FESS and the injected time delay can be identified accurately and promptly. With the proposed MPC scheme, the system frequency can reach the reference and remain stable rapidly in the presence of status feedback attacks and time-delay attacks.

6. Future work

For the MG attack model, it is assumed that the status feedback attacks only compromise the status of BESS/FESS and the time-delay attacks only intrude the communication channel between sensors and controllers. However, FDI attack can be implemented on the other part of MG (e.g. PMU) and forward time-delay attacks from controllers to

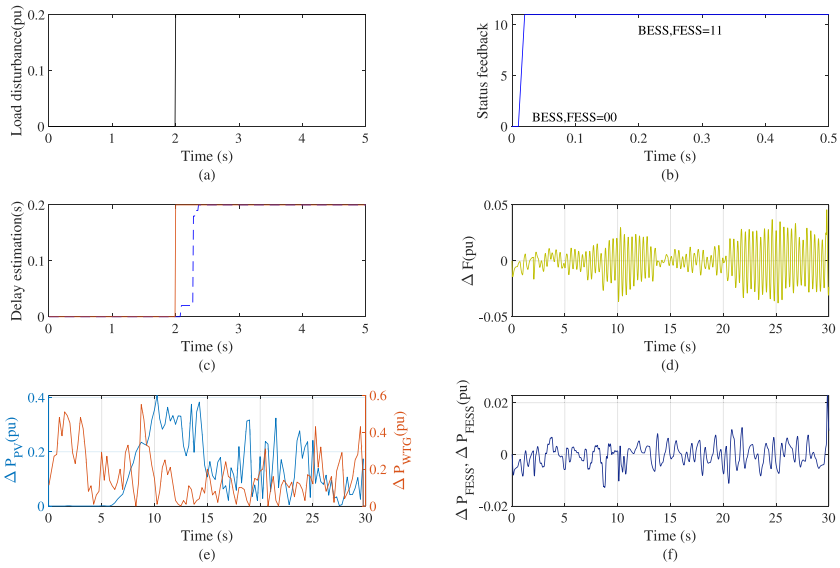

Fig. 16. The performance result in Case 5. (a) Load disturbance. (b) Online status feedback. (c) GCC time delay estimation. (d) Frequency response. (e) The PV and WTG output power. (f) The output power of BESS/FESS.

the plant should be possible in real life. Moreover, frequency regulation of the MG is confined to linear and time-invariant dynamics of the system. The proposed defense schemes are not equipped to handle nonlinear system dynamics or complex networked topology. The MPC controller in this paper is designed to control the generation of DEG and FC for the secondary frequency control. Detailed extension of the control to the ESS considering cyberattacks for frequency regulation will be promising to further improve the resilience of the system against the cyberattacks. For future work, more detailed MG models considering more accurate modeling of the ESS, FC and DEG can be studied and the control strategy can be improved by data-driven methods. Meanwhile, more complex MG configuration, e.g., networked microgrids, will be analyzed. Tuning the parameters to improve the performance of MPC controller can be studied. A more comprehensive mitigation method and robustness analysis of MG under other types of cyberattacks, e.g., DoS attacks, is also suggested.

CRediT authorship contribution statement

Zhengrong Chen: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Data curation, Writing – original draft, Visualization. **Zhaoxi Liu:** Conceptualization, Methodology, Validation, Formal analysis, Writing – review & editing. **Lingfeng Wang:** Conceptualization, Methodology, Resources, Writing – review & editing, Supervision, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation Industry/University Cooperative Research Center on Grid-connected Advanced Power Electronic Systems (GRAPES) under Award GR-18-06.

References

[1] Hatziargyriou N, Asano H, Iravani R, Marnay C. Microgrids. IEEE Power Energy Mag 2007;5(4):78–94.
[2] Zayegh OA. Recent developments in microgrids and example cases around the world—A review. Renew Sustain Energy Rev 2011.
[3] Hirsch A, Parag Y, Guerrero J. Microgrids: A review of technologies, key drivers, and outstanding issues. Renew Sustain Energy Rev 2018;90:402–11.
[4] Olivares DE, Mehrizi-Sani A, Etemadi AH, Cañizares CA, Iravani R, Kazerani M, et al. Trends in microgrid control. IEEE Trans Smart Grid 2014;5(4):1905–19.
[5] Bidram A, Davoudi A. Hierarchical structure of microgrids control system. IEEE Trans Smart Grid 2012;3(4):1963–76.
[6] Guerrero JM, Vasquez JC, Matas J, De Vicuña LG, Castilla M. Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization. IEEE Trans Ind Electron 2010;58(1):158–72.
[7] Guerrero JM, Chandorkar M, Lee T-L, Loh PC. Advanced control architectures for intelligent microgrids—Part I: Decentralized and hierarchical control. IEEE Trans Ind Electron 2012;60(4):1254–62.
[8] Rey JM, Martí P, Velasco M, Miret J, Castilla M. Secondary switched control with no communications for islanded microgrids. IEEE Trans Ind Electron 2017;64(11):8534–45.
[9] Han R, Meng L, Guerrero JM, Vasquez JC. Distributed nonlinear control with event-triggered communication to achieve current-sharing and voltage regulation in DC microgrids. IEEE Trans Power Electron 2017;33(7):6416–33.
[10] Bevrani H, Habibi F, Babahajyani P, Watanabe M, Mitani Y. Intelligent frequency control in an AC microgrid: Online PSO-based fuzzy tuning approach. IEEE Trans Smart Grid 2012;3(4):1935–44.
[11] Yi Z, Xu Y, Gu W, Fei Z. Distributed model predictive control based secondary frequency regulation for a microgrid with massive distributed resources. IEEE Trans Sustain Energy 2020;12(2):1078–89.
[12] John T, Lam SP. Voltage and frequency control during microgrid islanding in a multi-area multi-microgrid system. IET Gener Transm Distrib 2017;11(6):1502–12.
[13] Ersdal AM, Imsland L, Uhlen K. Model predictive load-frequency control. IEEE Trans Power Syst 2015;31(1):777–85.
[14] Liu K, Liu T, Tang Z, Hill DJ. Distributed MPC-based frequency control in networked microgrids with voltage constraints. IEEE Trans Smart Grid 2019;10(6):6343–54.
[15] Ahumada C, Cárdenas R, Saez D, Guerrero JM. Secondary control strategies for frequency restoration in islanded microgrids with consideration of communication delays. IEEE Trans Smart Grid 2015;7(3):1430–41.
[16] Industrial control systems are still vulnerable to malicious cyberattacks. Website; 2019, https://www.technologyreview.com/2019/01/28/137704/industrial-control-systems-are-still-vulnerable-to-malicious-cyberattacks/.
[17] Lee RM, Assante MJ, Conway T. Analysis of the cyber attack on the Ukrainian power grid. Electr Inf Shar Anal Cent (E-ISAC) 2016;388.
[18] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur 2011;14(1):1–33.
[19] Liang G, Zhao J, Luo F, Weller SR, Dong ZY. A review of false data injection attacks against modern power systems. IEEE Trans Smart Grid 2016;8(4):1630–8.

[20] Liu S, Liu XP, El Saddik A. Denial-of-service (DoS) attacks on load frequency control in smart grids. In: Proc. 2013 IEEE PES innovative smart grid technologies conference (ISGT). IEEE; 2013, p. 1–6.
[21] Zhong X, Jayawardene I, Venayagamoorthy GK, Brooks R. Denial of service attack on tie-line bias control in a power system with PV plant. IEEE Trans Emerg Top Comput Intell 2017;1(5):375–90.
[22] Sargolzaei A, Yen KK, Abdelghani M. Time-delay switch attack on load frequency control in smart grid. Adv Commun Technol 2013;5:55–64.
[23] De Pace G, Wang Z, Benin J, He H, Sun YL. Evaluation of communication delay based attack against the smart grid. In: Proc. 2020 IEEE kansas power and energy conference (KPEC). IEEE; 2020, p. 1–6.
[24] Liu C, Bak CL, Chen Z, Lund P. Dynamic security assessment of western danish power system based on ensemble decision trees. In: Proc. 12th IET International Conference on Developments in Power System Protection (DPSP 2014). 2014, pp. 1–6.
[25] Teixeira A, Pérez D, Sandberg H, Johansson KH. Attack models and scenarios for networked control systems. In: 1st ACM international conference on high confidence networked systems (HiCoNS'12). Beijing, China: ACM; 2012, p. 55–64.
[26] Bi W, Zhang K, Yuan K, Wang Y, Chen C, Wang K. Observer-based attack detection and mitigation for load frequency control system. In: Proc. 2019 IEEE power & energy society general meeting (PESGM). IEEE; 2019, p. 1–5.
[27] Sridhar S, Govindarasu M. Model-based attack detection and mitigation for automatic generation control. IEEE Trans Smart Grid 2014;5(2):580–91.
[28] Abbaspour A, Sargolzaei A, Forouzannezhad P, Yen KK, Sarwat AI. Resilient control design for load frequency control system under false data injection attacks. IEEE Trans Ind Electron 2020;67(9):7951–62.
[29] Li Y, Huang R, Ma L. False data injection attack and defense method on load frequency control. IEEE Internet Things J 2021;8(4):2910–9.
[30] Lou X, Tran C, Tan R, Yau DKY, Kalbarczyk ZT, Banerjee AK, et al. Assessing and mitigating impact of time delay attack: Case studies for power grid controls. IEEE J Sel Areas Commun 2020;38(1):141–55.
[31] Lou X, Tran C, Yau DK, Tan R, Ng H, Fu TZ, et al. Learning-based time delay attack characterization for cyber-physical systems. In: Proc. 2019 IEEE international conference on communications, control, and computing technologies for smart grids (SmartGridComm). IEEE; 2019, p. 1–6.
[32] Gao B, Shi L. Modeling an attack-mitigation dynamic game-theoretic scheme for security vulnerability analysis in a cyber-physical power system. IEEE Access 2020;8:30322–31.
[33] Jeong H-s, Lee C-w. Time delay control with state feedback for azimuth motion of the frictionless positioning device. IEEE/ASME Trans Mechatronics 1997;2(3):161–8.
[34] Youcef-Toumi K, Ito O. A time delay controller for systems with unknown dynamics. J Dyn Syst Meas Control Trans ASME 1990;112(1):133–42.
[35] Sargolzaei A, Yen KK, Abdelghani MN, Mehbodniya A, Sargolzaei S, et al. A novel technique for detection of time delay switch attack on load frequency control. Intell Control Autom 2015;6(04):205.
[36] Obara S. Analysis of a fuel cell micro-grid with a small-scale wind turbine generator. Int J Hydrogen Energy 2007;32(3):323–36.
[37] Lee D-J, Wang L. Small-signal stability analysis of an autonomous hybrid renewable energy power generation/energy storage system part I: Time-domain simulations. IEEE Trans Energy Convers 2008;23(1):311–20.
[38] Senjyu T, Nakaji T, Uezato K, Funabashi T. A hybrid power system using alternative energy facilities in isolated island. IEEE Trans Energy Convers 2005;20(2):406–14.
[39] Kouro S, Cortes P, Vargas R, Ammann U, Rodriguez J. Model predictive control—A simple and powerful method to control power converters. IEEE Trans Ind Electron 2009;56(6):1826–38.
[40] Shadmand M, Balog R, Abu-Rub H. Model predictive control of PV sources in a smart DC distribution system: Maximum power point tracking and droop control. IEEE Trans Energy Convers 2014;29(4):913–21.
[41] Ma M, Zhang C, Liu X, Chen H. Distributed model predictive load frequency control of the multi-area power system after deregulation. IEEE Trans Ind Electron 2016;64(6):5129–39.
[42] Ye L, Zhang C, Tang Y, Zhong W, Zhao Y, Lu P, et al. Hierarchical model predictive control strategy based on dynamic active power dispatch for wind power cluster integration. IEEE Trans Power Syst 2019;34(6):4617–29.
[43] Hua H, Cao J, Yang G, Ren G. Voltage control for uncertain stochastic nonlinear system with application to energy internet: Non-fragile robust H∞ approach. J Math Anal Appl 2018;463(1):93–110.
[44] Hua H, Qin Y, He Z, Li L, Cao J. Energy sharing and frequency regulation in energy internet via mixed H2/H∞ control with Markovian jump. CSEE J Power Energy Syst 2020.
[45] Knapp C, Carter G. The generalized correlation method for estimation of time delay. IEEE Trans Acoust Speech Signal Process 1976.
[46] Azaria M, Hertz D. Time delay estimation by generalized cross correlation methods. IEEE Trans Acoust Speech Signal Process 1984;32(2):280–5.