MODEL PREDICTIVE CONTROL – BASED VIRTUAL ENERGY STORAGE SYSTEM FOR VIRTUAL INERTIA CONTROL AND FREQUENCY REGULATION IN MICROGRID UNDER CYBER ATTACKS

SATAWAT MUANGCHUEN

A Dissertation Submitted to University of Phayao

in Partial Fulfillment of the Requirements

for the Doctor of Philosophy Degree in Electrical Engineering

May 2024

แบบจำลองการควบคุมเชิงทำนายของระบบจัดเก็บพลังงานเสมือน สำหรับการควบคุมแรงเฉื่อยเสมือน และการปรับความถี่ในไมโครกริด ภายใต้การโจมตีทางไซเบอร์

ศตวรรษ เมืองชื่น

วิทยานิพนธ์เสนอมหาวิทยาลัยพะเยา เพื่อเป็นส่วนหนึ่งของการศึกษา
หลักสูตรปริญญาปรัชญาดุษฎีบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
พฤษภาคม 2567

MODEL PREDICTIVE CONTROL – BASED VIRTUAL ENERGY STORAGE SYSTEM FOR VIRTUAL INERTIA CONTROL AND FREQUENCY REGULATION IN MICROGRID UNDER CYBER ATTACKS

SATAWAT MUANGCHUEN

A Dissertation Submitted to University of Phayao

in Partial Fulfillment of the Requirements

for the Doctor of Philosophy Degree in Electrical Engineering

May 2024

Dissertation

Title

MODEL PREDICTIVE CONTROL – BASED VIRTUAL ENERGY STORAGE SYSTEM FOR VIRTUAL INERTIA CONTROL AND FREQUENCY REGULATION IN MICROGRID UNDER CYBER ATTACKS

Submitted by SATAWAT MUANGCHUEN

Approved in partial fulfillment of the requriements for the
Doctor of Philosophy Degree in Electrical Engineering
University of Phayao

Approved by

---------- Chairman
(Associate Professor Sanchai Dechanupaprittha , Ph.D.)

---------- Advisor
(Associate Professor Jonglak Pahasa , Ph.D.)

---------- Co Advisor
(Associate Professor Chawasak Rakpenthai , Ph.D.)

---------- Co Advisor
(Associate Professor Sermsak Uatrongjit , Ph.D.)

---------- External Examiner
(Associate Professor Sitthidet Vachirasricirikul , Ph.D.)

---------- Dean of School of Engineering
(Associate Professor Nattapong Damrongwiriyanupap , Ph.D.)

Title: MODEL PREDICTIVE CONTROL – BASED VIRTUAL ENERGY STORAGE SYSTEM FOR VIRTUAL INERTIA CONTROL AND FREQUENCY REGULATION IN MICROGRID UNDER CYBER ATTACKS

Author: Satawat Muangchuen, Dissertation: Ph.D. (Electrical Engineering), University of Phayao, 2023

Advisor: Associate Professor Jonglak Pahasa , Ph.D. Co–advisor Associate ProfessorChawasak Rakpenthai , Ph.D. Associate ProfessorSermsak Uatrongjit , Ph.D.

Keywords: Model Predictive Control, Virtual Energy Storage System, Virtual Inertia, Frequency Regulation, Microgrid, Cyber Attacks

ABSTRACT

This dissertation proposes the applications of model predictive control (MPC) – based virtual energy storage system (VESS) for virtual inertia control and frequency regulation under denial – of – service (DoS) attacks. Firstly, an improved resilient MPC (IR – MPC) – based VESS is introduced for enhancing microgrid virtual inertia control under DoS attacks. IR – MPC comprises an attack detector, an autoregressive (AR) – based signal estimator, and an MPC – based VESS controller. An attack detector was used to detect the DoS attacks. An AR – based signal estimator is then used to estimate the feedback data that are subjected to DoS attacks. Then, an enhanced resilient MPC (ER – MPC) is presented for controlling proton exchange membrane electrolyzers (PEMEL) to regulate frequency under severe DoS attacks. The proposed ER – MPC consists of (1) the combination of AR model – based prediction and hold signal methods which are used to reconstruct attacked signals during severe DoS attacks, and (2) an MPC – based computation of control signal for the PEMEL stack. The simulation results revealed that under a DoS attack, the proposed IR – MPC and ER – MPC can successfully improve the microgrid virtual inertia emulation and frequency regulation. Additionally, the proposed IR – MPC and ER – MPC have a performance effect over the compared techniques in terms of the reduction in rate of change of frequency (RoCoF) deviation and frequency deviation during normal situations, DoS attacks, and disconnection of wind turbine generation.

ACKNOWLEDGEMENT

This dissertation has been completed with great success. Received exceptional help and support from numerous sources, especially from Associate Professor Dr. Jonglak Pahasa, their dissertation advisor. She provided invaluable guidance and consistently monitored and tracked research progress. The researcher is deeply grateful for the professor's generosity and wants to express heartfelt thanks to this remarkable opportunity.

I respectfully express my gratitude to the knowledgeable and experienced individuals who generously dedicated their valuable time to reviewing and providing suggestions, recommendations, and serving as dissertation examiners.

I would like to express my heartfelt gratitude to the President of Phayao University, the Dean of the Faculty of Engineering, and the university staff for their kind assistance in reviewing the accuracy of this dissertation.

Furthermore, the student has also received assistance and encouragement from family members and numerous individuals, whose contributions cannot be fully mentioned here. The researcher appreciates and is profoundly grateful for the kindness and goodwill of everyone involved. Therefore, I extend my heartfelt gratitude for this opportunity.

Satawat Muangchuen

LIST OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER I

INTRODUCTION

Background and Rational of the Study

Currently, there has been a significant rise in the demand for electricity across numerous countries worldwide. This increase can be attributed to factors such as a growing population, economic growth, and the essential role electricity plays in the industry. However, most of the electricity consumed comes from non – renewable fossil fuels, which are finite resources. As a result, many countries have shifted their focus towards renewable energy sources like wind and solar power to generate more electricity and reduce their reliance on fossil fuels due to their unpredictable nature. However, the utilization of these renewable energy sources in power systems can affect the stability of their voltage and frequency in the power system. This is because the amount of energy produced from renewable energy sources is subject to weather conditions, making it difficult to match electricity production with consumption demand. To address this, microgrids are employed, which help to enhance the efficiency of controlling and stabilizing the system compared to traditional power systems. A microgrid is a low or medium voltage system that integrates small – scale power generation, load management, and advanced communication systems. Microgrids offer increased flexibility and control over the power system and improved reliability and resilience against power outages. The various components of a microgrid function seamlessly as a single system connected to the main power grid. Even in emergency situations when disconnected from the main power grid, the fundamental principle of microgrid electricity production is to balance power production with internal demand and utilize the main power grid to maintain stability.

Microgrids that use renewable energy sources, such as solar and wind power, to generate electricity for homes, factories, and other users must consider the stability and balance of the system. The system must ensure that the voltage and frequency of the electricity are stable to prevent damage to equipment and ensure the safety of

the users. The balance of the system can be affected by changes in weather conditions or changes in demand, and adjustments may be needed to ensure that the system remains stable. Microgrids can also operate independently from the main grid during power outages, providing a reliable source of electricity to users. Microgrids that use electric power from renewable energy sources, such as wind and solar power for factories, households, or other energy needs, must consider the maintenance of stability in various aspects to ensure reliability. This includes maintaining a balance between power production and the power demand within the system and utilizing the main power grid to enhance stability. However, the fluctuating nature of renewable energy sources and changing energy needs make it difficult to maintain balance and stability without proper control. Therefore, a control system is necessary to reduce the impact of these imbalances and maintain the frequency and voltage within standard values even with changes in power production and demand. The problem of controlling the power system can be divided into two main topics: controlling the actual power to maintain the level of frequency and controlling the reactive power to maintain the level of voltage. The control of actual power is also known as "frequency load control." The most important role of frequency load control is to maintain the frequency constant despite changes in power load or power generation from renewable energy sources which can vary in short periods, making it difficult for the main power plants to respond promptly. Without control, the system becomes unstable, resulting in equipment damage and potential blackout. To maintain balance, an automatic control system is required to adjust the power output of the main power plants and other regulating devices. Currently, the use of renewable energy systems to produce electricity has gained significant interest. When these systems are connected to the main electricity grid, they can cause disturbances due to the uncertainty of the electricity generated by renewable sources. This is caused by changes in power from renewable energy sources, which are dependent on various environmental factors. Consequently, controlling the load frequency becomes more difficult and less effective.

The research demonstrated a decrease in the influence of fluctuations originating from renewable energy sources as well as the consequences of the model predictive control employed in the virtual energy storage system. Virtual inertia and frequency management were simulated in conjunction with the microgrid. The study utilized reachability methods to evaluate the impact of cyberattacks on the load frequency control (LFC) system, considering the scenario of malicious actors controlling the control centers. The predictive capability of the virtual energy storage system was employed to analyze the predicted energy changes. The observed trend was then implemented as an input to the control system, where the current power factor was used to determine a suitable control signal. The results of this control system were compared with those of the PI controller system.

The purposes of the study

1. To develop the improved model predictive control of the virtual energy storage system.
2. To study virtual inertia control for microgrid.
3. To improve the frequency regulation under cyberattacks of microgrids.

Research Question

How can the stability and reliability of microgrids powered by renewable energy sources be enhanced in the face of fluctuating energy production and what role does predictive control and virtual energy storage play in achieving this while considering cybersecurity concerns.

Research Scope

1. Consider the operation of the microgrids, which includes the generation of electricity from Wind turbines, Photovoltaic and Thermal power plants.
2. The predictions applied in conjunction with the analysis are of acceptable accuracy.
3. MATLAB/Simulink program has been used for simulation experiment.

Research Methods

1. Study method of load frequency control for a microgrids.

2. Study model predictive control algorithm.

3. Study the virtual energy storge system for microgrid virtual inertia control.

4. Study the frequency regulation under cyberattacks.

5. Develop the programs (MATLAB/Simulink) for the control virtual energy storge system for microgrid virtual inertia control and frequency regulation under cyberattacks.

6. Test the performances of the proposed algorithms in term of accurate, robustness and computation time.

Expected Benefits

1. Increased knowledge and understanding of frequency control techniques in microgrids.

2. Enhanced knowledge and understanding of power forecasting and its application to load frequency control.

3. Development of load frequency control improvement techniques using a forecasting model of microgrid power with hybrid renewable energy sources.

4. Increased knowledge and understanding of cybersecurity defense in microgrids.

Research Duration

The research plan lasted approximately one year. The plan of the year is to review and study the literature related to model predictive control – based virtual energy storage systems, microgrids, virtual inertia control, and frequency regulation under cyberattacks, details of the works in Table 1.

Table 1 One year research plan.

Detail of work	Month											
	1	2	3	4	5	6	7	8	9	10	11	12
1. Reviews and research related to load frequency control.												
2. Study mathematical model of load frequency control for a microgrid.												
3. Study model predictive control algorithm.												
4. Study MATLAB/Simulink programming												
5. Develop simulation program for:												
– Model Predictive Control												
– Virtual Energy Storge System												
– Virtual Inertia Control												
– Frequency Regulation under cyberattacks												
6. Organize a seminar to present the progress of work.												
7. Test the Model Predictive Control – based Virtual Energy Storge System.												
8. Prepare paper to present at the academic meetings and/or publishing in international journal.												
9. Organize a seminar to present the progress of work.												
10. Prepare Ph.D. dissertation.												
11. Dissertation examination.												
12. Dissertation correction.												

CHAPTER II

REVIEW OF RELATED LITERATURE AND RESEARCH

Virtual Energy Storage System

A virtual energy storage system (VESS) that combines a demand response and energy storage system was developed to support the distribution network voltage, enabling more distributed generators (DG) integration. The VESS concept and its potential applications are introduced, followed by an explanation of the modeling and control of the VESS components and VESS control scheme. A population of industrial bitumen tanks and battery energy storage systems were used to demonstrate the performance of the proposed voltage control scheme of the VESS. Two types of DG, solar and wind generation and the VESS, are connected to a medium – voltage network of the United Kingdom generic distribution system (UKGDS). The VESS control scheme operates cooperatively with on – load tap changers to prevent voltage hunt. The effectiveness of the proposed VESS control was assessed through time – series analysis over different seasons of the year.

A virtual energy storage system integrates various controllable components of an energy system into a unified entity that functions similarly to a large – scale energy storage system with lower capital expenses. Examples of such components include flexible loads with thermal storage, such as electric heaters, and distributed generation systems, such as combined heat and power (CHP) units or conventional energy storage systems. The VESS enables these components to participate in the electricity and ancillary markets to provide transmission and distribution level services [1].

Potential Applications

A VESS can form a synthetic Energy storage system (ESS) at both the transmission and distribution levels with varying capacities owing to the aggregation. In the "hybrid urban energy storage" project [2], various distributed energy systems in

buildings (e.g., heat pumps or combined heat and power systems (CHPs)), as well as central and decentral energy storage systems, are coordinated to create a VESS. This system utilizes the existing potential of energy balancing components in cities for grid ancillary services at a reduced cost. Thus, a VESS exhibits the characteristics of both a high – power – rating ESS and a high – energy – rating ESS, making it suitable for a wide range of applications. Based on the guidelines of the National Infrastructure Commission, the potential capabilities of a VESS are listed below:

1. Facilitate the integration of renewable energy sources (RESs) in the distribution networks. A VESS can charge/discharge to smooth the power output variations of renewable generation [3], [4]. Additionally, it can increase the distribution network hosting capacity for RESs [3], where the integration of RESs is limited by the voltage and thermal constraints.

2. Defer transmission networks reinforcements. A VESS can increase the utilization of transmission networks by providing immediate actions following a system contingency [5]. Additionally, a VESS can effectively mitigate the potential network congestions, and therefore postpones the transmission reinforcements.

3. Reduce generation margins. A VESS can reduce the required spinning reserve capacity and increase the generators loading capacity [6]. With smart grid technologies, the available VESS capacity can be reported to the system operator in advance and even every second [7].

4. Provide ancillary services. During system contingencies and system emergencies [8], A VESS can provide voltage support and frequency support. In addition, primary frequency response requirements which are at present mainly met by the costly frequency – sensitive generation is expected to increase by 30 – 40% in the next 5 years in the Great Britain (GB) power system. A VESS is technically feasible to provide such services because it is able to provide faster response, higher ramp rates and higher flexibilities than the conventional generating units [9].

These include but are not limited to, providing energy arbitrage, facilitating renewable integration in distribution network, deferring the transmission and distribution systems reinforcements, and providing ancillary services such as frequency response, voltage support and power quality improvements.

Virtual Energy Storage System Model

A simplified model of a battery energy storage system model was developed in [10], which consists of a generic battery model and a simplified power electronics model. The generic battery model shown in Figure 1 is composed of a controllable voltage source, a controllable current source, and a resistance connected in series. The charging and discharging characteristics are assumed similar. The simplified power electronic converter model is a first – order lag that represents delays in the converter control loop.

A VESS is formed to provide the required frequency response to the power system in order to participate in the Great Britain (GB) Firm Frequency Response (FFR) market as an aggregator. The FFR market is considered as the most lucrative ancillary services available on the MW basis in the GB power system [11].

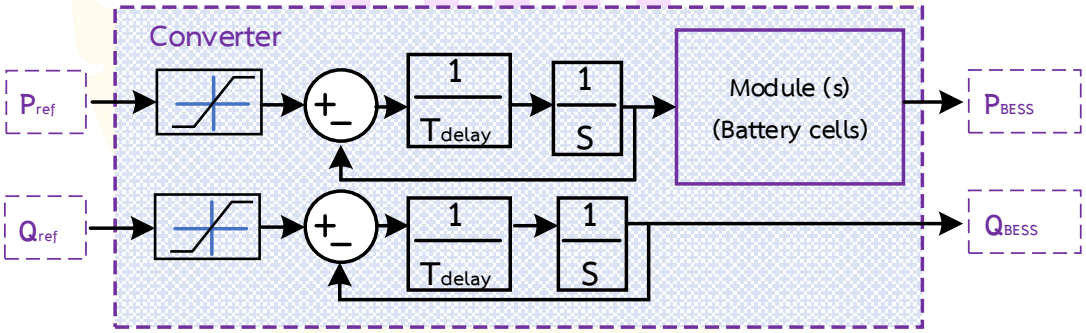


Figure 1 Simplified battery energy storage system model.

Source: Saif Sabah Sami, et al., 2018, p. 147

Voltage Control of Demand Response Units

A distributed voltage controller is added to the inherent temperature control of each bitumen tank (BT). The voltage controller alters the power consumption of the DR units – based on the local voltage measurements, as shown in Figure 2. The temperature control measures the temperature T of the tank and generates state signals S_T. The voltage control measures the bus voltage V and generates state signals S_{HV} and S_{LV}. The final switching signal S_{final} to the heater is then determined using logic gates, which ensure the priority of temperature control. Therefore, the extra voltage control does not undermine the hot storage function of the BTs.

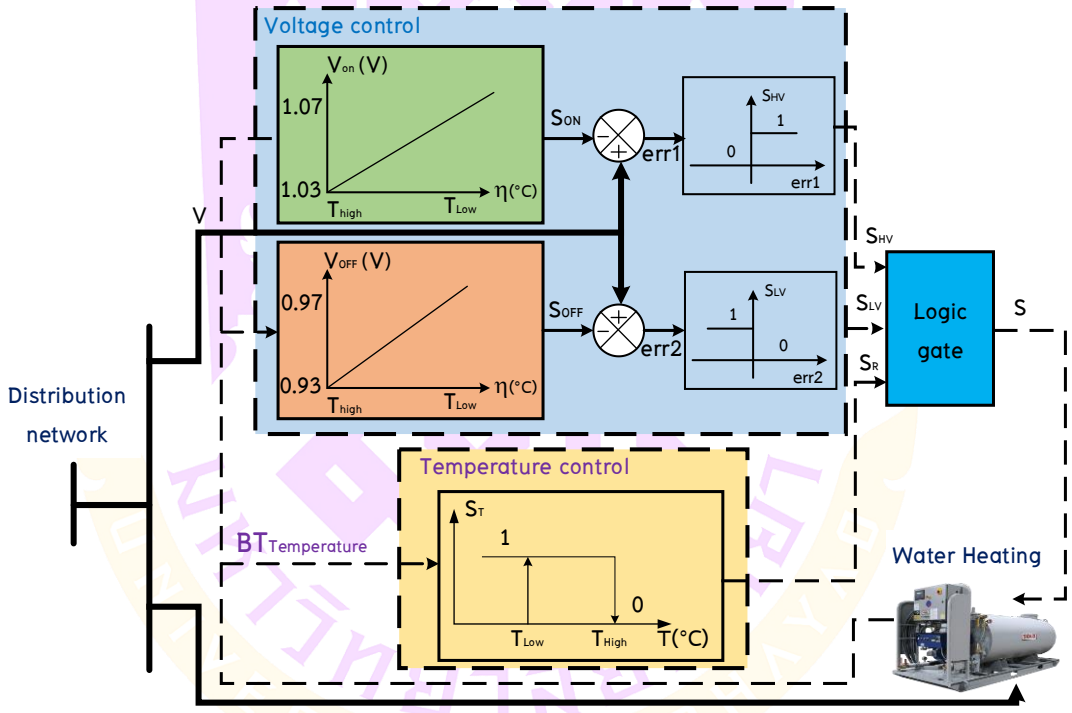


Figure 2 The control system of a flexible load.

Source: Saif Sabah Sami, et al., 2018, p. 148

The voltage control algorithm switches the load on/off in response to voltage deviations. The control algorithm assigns a pair of voltage setpoints, namely V_{ON} and V_{OFF}, which vary dynamically and linearly with the BT temperature. For example, a BT will have higher V_{ON} and lower V_{OFF} values if its temperature is higher than other BT temperatures. The control algorithm continuously compared the measured voltage (V) with the set points. If V is higher than V_{ON}, the voltage control generates a state signal S_{HV}, and the load is switched on. In contrast, if voltage V is lower than V_{OFF}, the voltage control generates a state signal S_{LV} and the load is switched off. The linear variation of V_{ON} and V_{OFF} with temperature ensures that among a population of BTs, following a voltage drop, the BT with the highest temperature will be switched off first because it is most willing to be switched off because its temperature has already been high.

In contrast, the BTs will be switched on in response to a voltage rise starting from the BT with the lowest temperature. Therefore, the number of BTs committed to responding to voltage deviations increases linearly with an increase in the voltage deviation. Hence, all the demand response units are committed if the voltage accessed the limits. It was assumed that the distribution network voltage limits follow the British Standard EN 50160, a distribution network with voltage limits of ±6% of nominal value (i.e. 0.94 p.u. – 1.06 p.u.), and voltage control dead – band of ±3% (i.e. 0.97 p.u. – 1.03 p.u.) were used. BTs have low and high temperature limits of 150°C and 180°C, respectively [1].

Voltage Control of Energy Storage System

Energy storage system (ESS) control methodology consists of main and supplementary controllers. The main controller drives the active and reactive power outputs of the ESS in response to voltage violations. The supplementary controller maintains the ESS's state of charge value within a certain range, which facilitates a secure, sustainable and efficient operation. The active and reactive power outputs of the energy storage system were determined using droop control, and the droop setting was obtained – based on the voltage sensitivity factor matrices.

1. The voltage sensitivity factors match the voltage sensitivity factors that relate the change in voltage at a bus to a change in active and/or reactive power (s) at other buses in the network [12]. In a voltage sensitivity factor matrix, a high voltage sensitivity factor implies that a change in active and reactive power at a bus drives a large change in voltage at the corresponding bus. The voltage sensitivity factor matrices Equations (2) – (4) are extracted from the Jacobian matrix in Equation (1).

$$\begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} = \begin{bmatrix} \frac{\partial P}{\partial \delta} & \frac{\partial P}{\partial V} \\ \frac{\partial Q}{\partial \delta} & \frac{\partial Q}{\partial V} \end{bmatrix} \begin{bmatrix} \Delta \delta \\ \Delta V \end{bmatrix} \tag{1}$$

$$\Delta V = M \cdot \Delta P + N \cdot \Delta Q \tag{2}$$

$$M = \left[\frac{\partial P}{\partial V} - \frac{\partial P}{\partial \delta} \cdot \left[\frac{\partial Q}{\partial \delta} \right]^{-1} \cdot \frac{\partial Q}{\partial V} \right]^{-1} \tag{3}$$

$$N = -M \cdot \frac{\partial P}{\partial \delta} \cdot \left[\frac{\partial Q}{\partial \delta} \right]^{-1} \tag{4}$$

2. Droop control of energy storage systems using voltage sensitivity factors. A concise network analysis is conducted to identify the buses that are most susceptible to voltage infractions. These buses are often heavily loaded, connected to a large amount of DG, or connected through small – capacity branches. These buses are equipped with remote monitoring devices to monitor and send voltage values to the ESS controller. The ESS controller receives the voltages of the buses and classifies them into zones – based on British standard EN 50160, as illustrated in Figure 3.

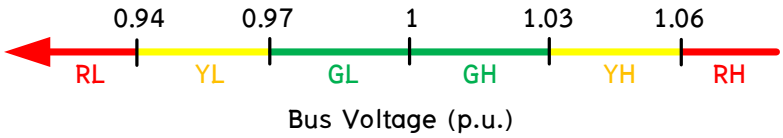


Figure 3 Classified bus voltage zones.

Source: Saif Sabah Sami, et al., 2018, p. 149

2.1 Red zones (RH and RL) represent the voltage violation ranges, that is, bus voltage violates/exceeds the ±6% limits.

2.2 Yellow zones (YL and YH) represent the severe voltage deviation ranges, that is, the bus voltage largely deviates (equal to or larger than ±3%) from the nominal value, yet within the limits.

2.3 Green zones (GL and GH) represent the slight voltage deviation ranges, that is, the bus voltage deviates marginally (smaller than ±3%) from the nominal value.

3. Supplementary Control of Energy Storage System When all monitored bus voltages are in the green zones (Figure 3), the ESS supplementary control restores the state of charge to 50 ±10%. The ESS charges/discharges using droop control with respect to the monitored bus with the highest voltage – sensitivity factors. The ESS responds with sufficient power to push the bus voltage to the yellow zone (Figure 3). This ensures that the consuming ESS power will not cause voltage violations. Only the active power of Equation (5) is used and the reactive power is set to zero. Consequently, any forthcoming charging or discharging requirements are expected to be satisfied.

$$\Delta V_i = M_{iESS} \times \Delta P_{ESS} + N_{iESS} \times \Delta Q_{ESS} \quad (5)$$

where

M_{iESS} is the voltage sensitivity factor relating the change in the ESS active power to the change in bus i voltage,

N_{iESS} is the voltage sensitivity factor relating the change in ESS reactive power to the change in bus i voltage.

Coordinated Voltage Control of VESS

The coordination between demand response and energy storage system in the VESS is achieved by setting their controllers with different time delay constraints. As a result, they will not conflict with each other and cause voltage hunting. The time delay constant coordination also considers conventional voltage control equipment including the OLTC and voltage regulators (VR). When a voltage violation occurs, the voltage controllers of the demand response (DR) units respond first with a time delay constant τ_{DR}. If the voltage violation continues, the energy storage system (ESS) with a time delay constant τ_{ESS} (i.e. $\tau_{ESS} > \tau_{DR}$) will respond secondly. This procedure ensures that no voltage violation occurs because of the uncertainty of the demand response. If required, the on – load tap changer (OLTC) will take action last with a time delay constant τ_{OLTC} (i.e. $\tau_{OLTC} > \tau_{ESS}$). This, in turn, results in less OLTC actions [1].

Capacity of A Virtual Energy Storage System

The virtual energy storage considered here is a controllable load and controllable generation. The virtual energy storage capacity of the controllable load is shown in:

Figure 4 (a) [13]. When the virtual energy storage of the load consumes more power than the conventional load, the surplus power is the charging capacity. When the virtual energy storage of the load consumes less power than the conventional load, the release power is the discharge capacity.

Figure 4 (b) shows the virtual energy storage capacity of the controllable source (generator). When the virtual energy storage of the generator produces more power than a conventional generator (not virtual energy storage), the surplus power is the discharge capacity. When the virtual energy storage of the generator produces less power than that of the conventional generator, the released power is the charging capacity.

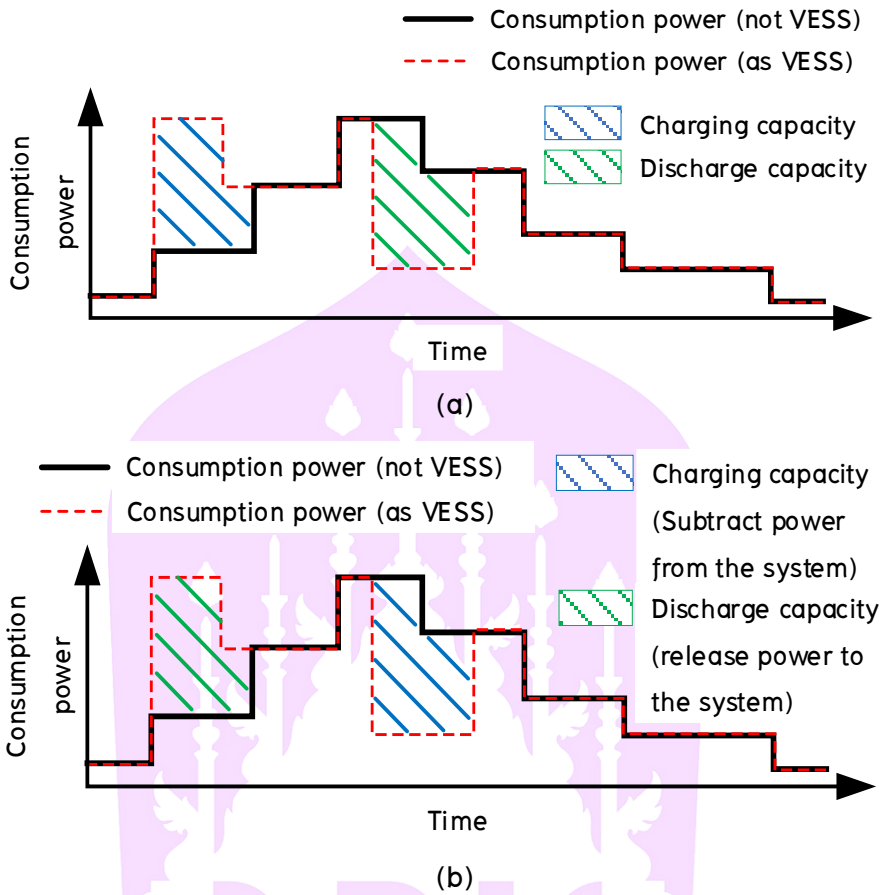


Figure 4 Virtual energy storage system capacity (a) controllable load (b) controllable source.

Source: Jonglak, Potejanasak and Issarachai, 2022, p. 133712

Emulate Virtual Inertia

In recent years, owing to increasing concern regarding the long – term adequacy of nonrenewable energy sources such as petroleum, coal, and natural gas, and the environmental problems caused by the utilization of those resources, including electricity generation, the penetration of renewable energy sources (RESs) in power systems has rapidly increased and has become a necessity.

The increasing concern in the aforementioned issue, followed by the changes in the energy regulation, makes the increasing penetration of RESs – based generation such as photovoltaic and wind turbine generation in the power system inevitable. For example, in Japan, up to 64 GW of photovoltaic is expected to be connected to the grid by 2030 [14]. In countries such as Denmark, Ireland, and Germany, an annual penetration level of RESs of more than 20% has been achieved at the national level [15]. At a global level, 2018, 103 GW of photovoltaic generation units were installed globally. With these additional installations, a total installed capacity of more than 512 GW was achieved in 2018 [16]. To enable the appropriate transfer of electrical energy from RESs to the power system, the inverter is normally required to integrate the RESs – based generation units into the power system. However, the inverter (and another power electronics interface in general) is inertia less, due to the absence of rotating mass as the source of inertia. Thus, the increasing penetration of inverter – based generation units implies a reduction in the system inertia. In the power system dominated by the inverter – based renewable generation units, the overall system inertia would be significantly lower compared to the traditional power system dominated by the traditional synchronous generators (SGs).

As a result, even though the rapid increase in the penetration level of inverter – based RESs generation units is beneficial from an environmental perspective and implies a better utilization of available sources of renewables, it is detrimental to the stability of the power system, particularly to the frequency stability [17] because the frequency stability of the system is closely related to the amount of inertia in the system [18]. An illustration of the correlation between inertia and frequency is shown in Figure 5, which clearly shows that with a lower system inertia, the frequency of NADIR subject to a frequency event would be lower.

In addition, other than the direct impact to the overall system inertia, the increasing penetration of RESs – based generation Units could also lead to negative effects such as excessive electricity supply in the system in the case of maximum electricity generation by RESs – based generation units, power fluctuation caused by variable nature of RESs, and the deterioration of frequency regulation [19].

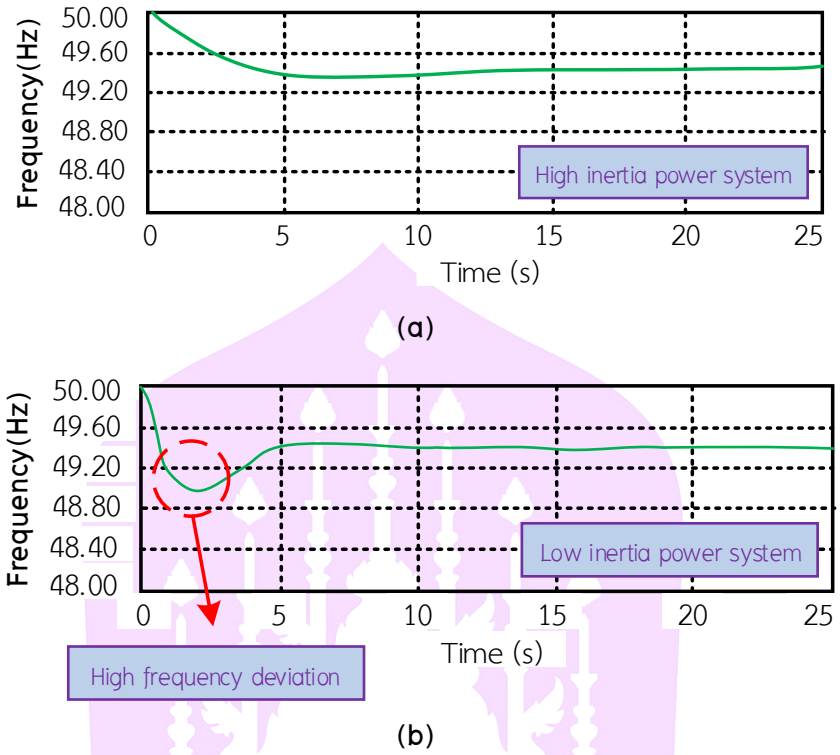


Figure 5 Illustration of the correlation between inertia and frequency: frequency response to a particular frequency event in the (a) high inertia power system and (b) low inertia power system.

Source: Thongchart, et al., 2021, p. 2

Therefore, to enable a high penetration of RESs in the power system, a new control strategy that could also provide the inertia support to the power system is developed. The control strategy is called a virtual inertia control. In general, the virtual inertia control is defined as the concept of providing virtual inertia to the power system by using an inverter, energy storage system (ESS), and proper control for virtual inertia emulation. This concept is also known as a virtual synchronous machine (VISMA) [20], virtual synchronous generator (VSG) [21], or synchronverter [22]. The aforementioned strategies have the same common objective, which is to provide additional inertia virtually by utilizing an inverter and an energy storage system (ESS), supported by a proper virtual

inertia control mechanism. Using the aforementioned strategies, the kinetic energy reservoir in the rotating mass of a conventional synchronous generator can be imitated on the inverter – based generator, thereby enabling the emulation of virtual inertia by the inverter – based generator.

Owing to their capability of providing additional inertia support in a low – inertia power system, virtual inertia control units would be an integral part of the future power system dominated by RESs. Thus, the V_{SG} is important to achieve a stable operation of the power system with high penetration of RESs – based generation units [23].

The implementation of a virtual inertia control is based on the emulation of the typical swing equation of a synchronous generator (SG) in the control of inverter. The typical swing equation of an SG can be expressed using Equation (6).

$$\overline{P}_m - \overline{P}_e = \overline{P}_a = \frac{2H}{\omega_0}\frac{d^2\delta}{dt^2} = \frac{2H}{\omega_0}\frac{d\Delta\omega_r}{dt} \tag{6}$$

where

$\overline{P}_m$ is mechanical power input [p.u.],
$\overline{P}_e$ is electrical power output [p.u.],
$\overline{P}_a$ is acceleration power [p.u.],
H is inertia constant [MW.s/MVA],
ω_0 is rated angular velocity of the rotor [rad/s],
ω_r is angular velocity of the rotor [rad/s],
δ is rotor angle [rad], and t is time [s],
$\overline{P}_m$ is related to the power supplied by the SG unit,
$\overline{P}_e$ is related to the load power demand.

When the damping component is included, the above equation becomes.

$$\overline{P}_m - \overline{P}_e = \frac{2H}{\omega_0}\frac{d\Delta\omega_r}{dt} + K_D\frac{\Delta\omega_r}{\omega_0} \tag{7}$$

where

K_D is the damping coefficient.

Equation (7) could also be represented in frequency (Hz) as

$$\overline{P}_m - \overline{P}_e = \frac{2H}{f_0}\frac{d\Delta f}{dt} + K_D\frac{\Delta f}{f_0} \quad (8)$$

where

f_0 is rated frequency of the power system [Hz],

f is the frequency of the power system [Hz].

The term $\frac{d\Delta f}{dt}$ is well known as the rate – of – change – of – frequency (RoCoF) of the power system. The swing equation shows the relationship between the active power and the angular rotor velocity of an SG and is also correlated to the system frequency, as the term $\frac{d^2\delta}{dt^2}$ indicates the change in system frequency or the angular rotor velocity of an SG. Based on the swing equation, the system frequency can increase or decrease depending on the balance between the mechanical power input P_m and the electrical power output P_e. When $(\overline{P}_m - \overline{P}_e)$ is positive, the acceleration power $\overline{P}_a$ is positive.

In this condition, system frequency will increase, and vice versa. At a steady – state operating point, the frequency was maintained by regulating the generation load balance using a speed – governing system in the SG units.

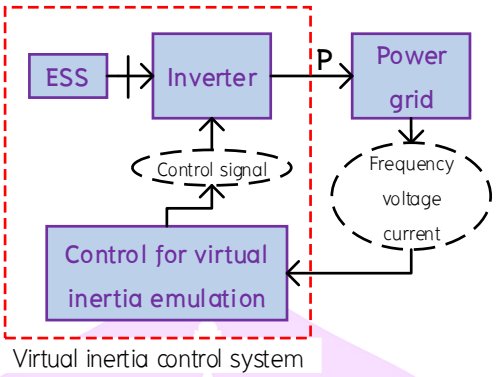


Figure 6 The basic diagram of virtual inertia control system.

Source: Thongchart, et al., 2021, p. 5

The development of the virtual inertia control is based on the swing equation described above. Various topologies have been proposed for emulating virtual inertia, as summarized in [24], [25]. However, all of these topologies have the same main objective: to provide the additional inertia virtually into the power system using the power electronics interface. The general concept of the virtual inertia control system is shown in Figure 6. In general, the virtual inertia control system consists of an energy source, the inverter, and proper control for virtual inertia emulation. The energy source in the virtual inertia control system is usually an ESS. Other energy sources, such as wind turbines, could also be used. The emulation of virtual inertia by using wind turbines (i.e. doubly fed induction generator (DFIGURE) wind turbines) is more commonly referred to as synthetic inertia. However, for better operational flexibility, an ESS should be used as an energy source.

The idea of virtual inertia is based on the implementation of the swing equation of an SG into the inverter of inverter – based RESs generation units so that the inverter (which is inertia – less) can be controlled to emulate the inertia characteristic of an SG. The term virtual inertia refers to the fact that the inertia characteristic of an SG is emulated without utilizing any kind of rotating mass. The control for virtual inertia emulation is used to determine the required inertia power output from the virtual inertia control system.

To emulate the virtual inertia, there are various available approaches to virtually emulate the inertia characteristic of an SG, as summarized in [19]. Among the available approaches, virtual emulation – based on the rate – of – change – of – frequency (RoCoF) of the system is the simplest and most fundamental method for emulating the virtual emulation – based on the RoCoF of the system. The virtual inertia power in this virtual inertia emulation method is calculated using Equation (9) based on Equation (8).

$$P_{VI} = K_{V1}\frac{d\Delta f}{dt} + K_D\Delta f \tag{9}$$

where

P_{VI} is output virtual inertia power of virtual inertia control units,

K_{V1} is virtual inertia constant gain.

In this method, the virtual inertia power of virtual inertia control units is directly emulated by using a derivative term ($d\Delta f / dt$). The virtual inertia can be emulated by simply incorporating derivative control into the controlled inverter – based on the frequency measurement of the system. The derivative control – based virtual inertia control is utilized in [26, 27] and the more advanced applications of the derivative control – based virtual inertia control are presented in [28].

Fundamental Virtual Inertia Synthesis and Control

The integration of distributed generators (DGs) and renewable energy sources (RESs) into traditional power system – based synchronous machines is immediately increasing owing to the energy crisis, environmental concerns, and economic growth. Together with the deployment of a modern (distributed) power system concept called the microgrids, such systems are suitable for integrating DGs/RESs into the distribution system [29]. Consequently, DGs/RESs have been developed into highly shared structures in modern power systems. Favorably, the consumers do not need to rely on the faraway traditional generation during a fault and they can have better power quality.

On the contrary, high DGs/RESs integration could cause critical frequency stability problems in the system as follows.

Firstly, a high DGs/RESs penetration curtails the number of traditional generating units, which directly contribute the initial response and reserve power for primary and secondary frequency control, resulting in larger frequency excursions and degradation of system stability and resiliency.

Secondly, the DGs/RESs – based generation naturally has nonexistent or low – inertia and damping properties due to the deployment of power electronics interfaces (i.e., inverters/converters). This power electronics interface has no rotating mass, which is the prominent ability in providing inertia and damping properties for slowing down the frequency change during a disturbance. The lack of system inertia and damping results in an increase in the rising rate – of – change – of – frequency (RoCoF), leading to abrupt frequency variations with larger amplitudes and load shedding, even at a small disturbance (see Figure 7). Accordingly, DGs/RESs – based generation may not engage in frequency control during normal system operations [30].

Therefore, penetrating DGs/RESs into the power system will undoubtedly lead to a reduction in the inertia and damping of the entire system, which can cause negative impacts on the power system dynamics, frequency/voltage regulation, and other operation and control issues. In the worst case, these problems can cause system instability, cascading failures, and power blackouts.

In response to the stability challenges driven by low system inertia and damping, a solution for stabilizing a modern power system is to synthesize additional inertia and damping virtually, allowing a high DGs/RESs participation in system operation [22]. Virtual inertia synthesis and control can be constructed by the short – term energy storage, power electronics converter/inverter, and advanced inertia control mechanism in the system that is called the virtual synchronous machine (VISMA) or virtual synchronous generator (VSG) concept [31]. The virtual inertia control system operates as a real synchronous machine/generator to provide virtual inertia and damping for short time intervals. Consequently, the idea of virtual inertia can be fundamental for regulating a large portion of DGs/RESs in today 'sand future power systems without compromising

system stability, reliability, and resiliency. Literature reviews, including past achievements on virtual inertia control and its applications, have been reported in [32]. The reports confirmed that the applications of virtual inertia control could offer uninterruptable power transfer between grid – connected and islanded operations.

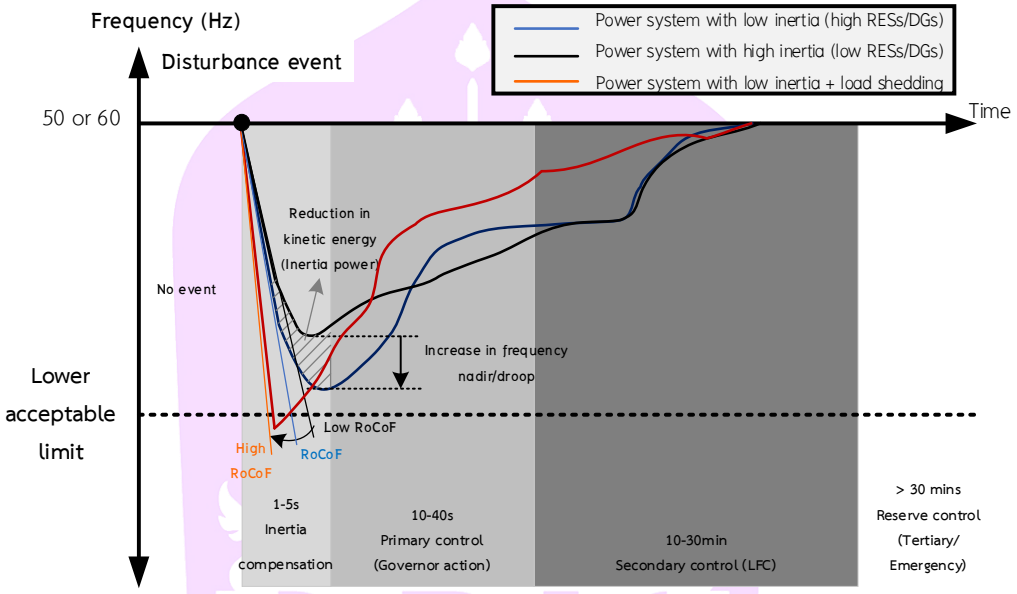


Figure 7 Comparison of frequency dynamic response between in modern power systems dominated by DGs/RESs and conventional power system dominated by synchronous generators.

Source: Thongchart, et al., 2021, p. 62

The principle of virtual inertia control can be implemented either to a single RESs/DG or a group of RESs/DGs. Implementing a single RES/DG might be suitable for individual owners of DG/RES. By implementing a group of DGs/RESs, it is easier and more economical to control in the network/grid aspect [19]. Figure 8 displays the fundamental structure of the virtual inertia control. It consists of an energy storage system (ESS), inverter, and inertia control mechanism. Then, the virtual inertia is synthesized into the system by regulating the active power via the inverter in inverse proportion to

the rotor speed. From the network point of view in regards to higher frequency noise triggered by switching of invertor's power transistors [33], it is noted that there is no difference between the electrical component of virtual inertia control and the electrical appearance of the electromechanical synchronous machine. Due to the inertia compensation principle, the virtual inertia control should absorb or inject active power; thus, the nominal state of charge (SoC) of the ESS in its system should be operated at 50% of its nominal capacity during a stationary (steady – state) circumstance. However, depending on the SoC situation, the operation of the virtual inertia control can be changed owing to the specified upper and lower limits (e.g., 20% for the lower limit and 80% for the upper limit). These limits can also be evaluated – based on the technology used in the ESS. During such limits, the virtual inertia control is operated in the inertia control mode when the energy in the system is lacking due to the unbalance between generation and load. However, the virtual inertia control is operated in the virtual load mode when the energy in the system is excess. Finally, the emulated power from a virtual inertia control unit can be expressed as [34]. It is noted that $d\Delta f / dt$ is the rate – of – change – of – frequency (RoCoF), f_0 is the nominal frequency of the system, K_{VI} is the virtual inertia characteristic/constant, D_{VI} is the virtual damping coefficient/constant, P_{Inv} is the nominal apparent power of the inverter unit, and P_0 is the primary power that transfers to the inverter.

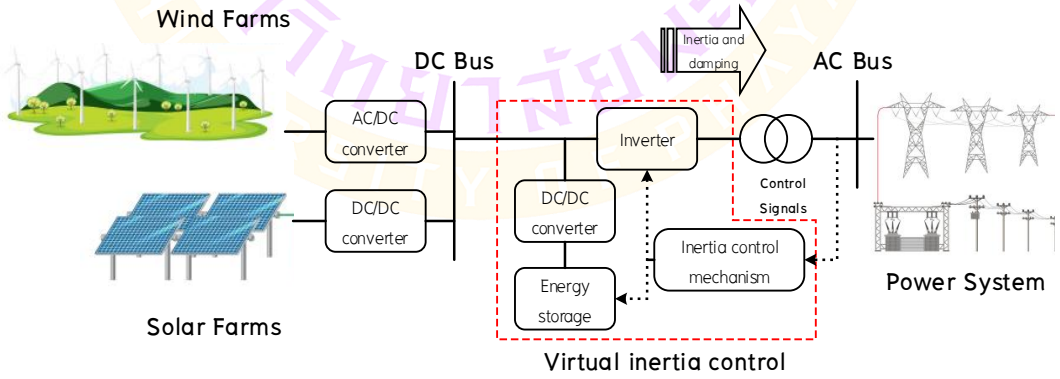


Figure 8 A fundamental concept and structure of virtual inertia control.

Generally, the initial rate of frequency variation presents the error signal with an equilibrium of zero; thus, the emulated power will be transferred only in the transient condition without restoring the system frequency to the nominal value. To deploy the frequency restoration ability for virtual inertia control, a frequency control droop must be added in terms of Equation (10). Considering Equation (11), the operation of the virtual inertia control can be explained in three main terms as follows:

$$P_{VI} = K_{VI}\left(d\frac{\Delta f}{dt}\right) + D_{VI}\left(\Delta f\right) + P_0 \tag{10}$$

$$K_{VI} = \frac{2HP_{Inv}}{f_0} \tag{11}$$

where

$\left(d\frac{\Delta f}{dt}\right)$ is the rate – of – change – of – frequency (RoCoF),

f_0 is the nominal frequency of the system,

K_{VI} is the virtual inertia characteristic/constant,

D_{VI} is the virtual damping coefficient/constant,

P_{Inv} is the nominal apparent power of the inverter unit,

P_0 is the primary power that transfers to the inverter.

The first term: which is known as the virtual inertia, can emulate the inertia behavior from a synchronous generator. This term decreases the maximum deviation of the rotor speed and curtail the system frequency nadir/overshoot after a disturbance. In this term, power is absorbed or generated by the negative or positive initial RoCoF.

The second term: which is known as the virtual damping, can emulate the damper windings effect of a synchronous generator. The D_{VI} must be selected so that the emulated power to be equal with the nominal power of the virtual inertia control system when the system frequency oscillation occurs at the specified maximum value. This term suppresses the oscillation of the system frequency after a disturbance, resulting in a faster stabilization time of the system.

The third term: represents the nominal primary power transferred to the inverter unit, generating constant power. In addition to K_{VI} and D_{VI}, they are negative constants that must be constant so that the virtual inertia system can exchange its maximum active power when the maximum specified frequency deviation and RoCoF occur. Increasing K_{VI} and D_{VI} indicates that more power will be absorbed or injected for a similar amount of RoCoF and frequency deviation. By combining these three terms, the virtual inertia control system is equally effective for electromechanical synchronous generators.

Considering a practical synchronous machine, the energy absorbed by the damping term is drained by the damping winding resistance. In the case of virtual inertia control, this power is consumed by the energy storage system to balance the power of the system.

To select a suitable energy storage type for inertia control, some important parameters must be considered, such as the power of the generating unit, maximum power of loads, averaged SoC during normal operation, operating time, and control delay [35].

Virtual Energy Storage System Using Inverter air conditioners and Photovoltaic Capacity

The IACs can be used as virtual energy storage all day. However, during the daytime (8.00 – 18.00h), the ambient temperature was very high. The virtual energy storage systems (VESS) charging capacity may not be sufficient for supporting virtual inertia and frequency regulation because of the high IAC power used to regulate the difference between the setting and ambient temperatures [14]. The PV generators can

support virtual inertia emulators and frequency regulation during the day. However, when the PV generator operates at maximum power generation, a reduced power generation VESS is performed. The VESS capacity was sufficient for supporting the virtual inertial emulator throughout the day.

PV and wind turbine generators can be used to reduce system inertia, as proposed in the literature [36]. Nevertheless, the main contribution of this study is the use of inverter air conditioners as the main component of virtual energy storage systems to provide virtual inertia and frequency regulation. Owing to the high ambient temperature during the daytime, the IAC may operate at maximum power consumption and may not provide sufficient power to support the virtual inertia emulator. Wind turbine generators were used as part of the virtual energy storage system in this study.

However, conventionally, the wind speed during the day is lower than that at night [37]. Wind power generation during the daytime may not be sufficient for frequency regulation in this study. Therefore, the PV generator is used in this work because PV generators operates in the daytime and can reduce power to support frequency regulation when the IACs cannot consume more power to regulate the microgrid frequency.

Frequency Regulation Concept

Frequency regulation is related to the energy balance between load demand and generation, which is of great significance and is recognized as a high – priority area by most operators [19]. Any disturbance that leads to an imbalance between the generation and load can cause an abrupt change in the system frequency, resulting in frequency oscillations. Frequency oscillations may affect system stability, operation, and resiliency. Large frequency oscillations can damage equipment, deteriorate load performance, overload transmission lines, trip protection relays, and, in the worst case, lead to system collapse and wide – area power blackouts.

The frequency of the system is proportional to the rotating speed of the generator. Thus, the frequency control issue may be directly transformed into a speed control issue for the generator turbine units. This problem was solved by applying a governing system that could track the generator speed and adjust the input value to

change the mechanical power output to follow the load variation and reduce the frequency deviation. Subsequently, the secondary control action restores the frequency to its nominal value.

Based on the frequency oscillation (deviation) territory, the natural response called inertia power compensation, along with primary control, secondary control, tertiary control, and emergency control may be needed to regulate system frequency. From Figure 9, f_0 is the nominal frequency (e.g., 50 Hz or 60 Hz), and Δf_1, Δf_2, Δf_3 and Δf_4 reveal frequency oscillation territories with respect to various operating conditions – based on permittable frequency operating standards [19].

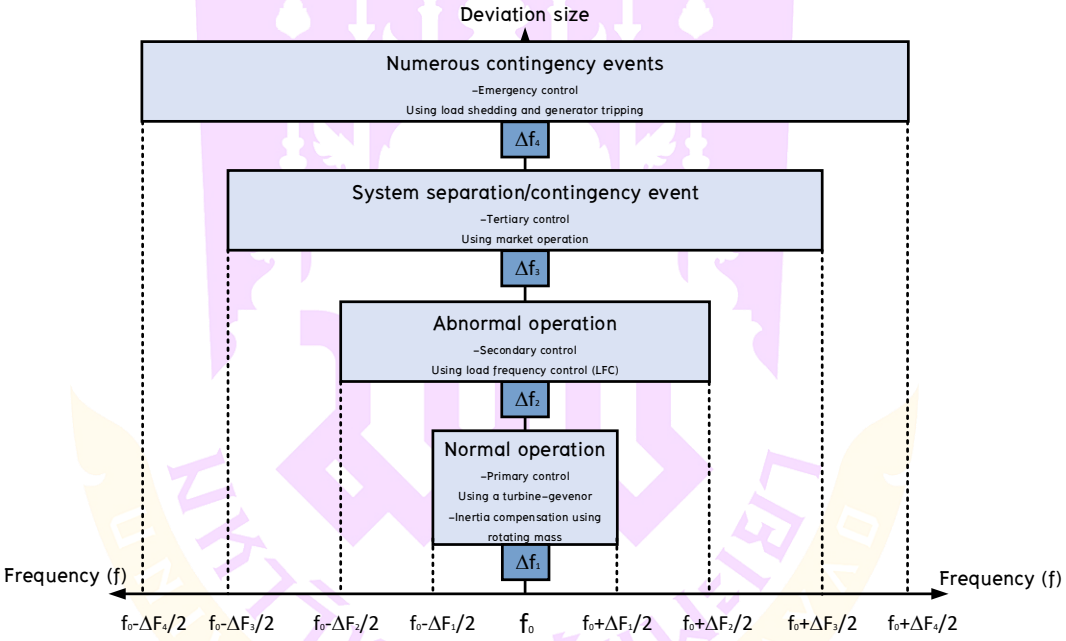


Figure 9 Operating control schemes with regards to frequency deviation size.

Source: Thongchart, et al., 2021, p. 14

During normal operation, the small frequency oscillations could be diminished by the inertia compensation and primary control. For larger frequency deviations (abnormal operation), based on the available reserve power, the secondary control can restore the system frequency back to the steady state or nominal value. For a critical load

generation mismatch with fast frequency variations during a significant disturbance/fault, the operation of secondary control may be insufficient to restore the system frequency back to the steady state. In such circumstances, it is necessary to activate the unusual operations of tertiary control, emergency control, and protection schemes, reducing the risk of cascading failures, load or grid/network separation events, and additional generation events [38].

Following a disturbance or event, the inertia power compensation in the rotating units respond within less than 10 second to arrest the initial frequency deviation. Then, the primary control loop in a governor – turbine unit is activated within 3 second and fully released to the system within 10 second. This service will be maintained, where necessary, up to 20–40 second. As soon as the system is stable, the system frequency recovers back to a fixed value, but it might be distinct from the nominal value as the generator droop generates a proportional type of action. Then, the secondary control is activated following the inertia compensation and primary control timescales and can be activated up to 30 minutes after a disturbance. This control can reestablish the nominal frequency and interchanged power by a distribution of the controlling power. In some critical disturbances or events, if the system frequency rapidly drops and reaches a decisive value, the tertiary and emergency controls are significantly needed to recover the frequency. If such actions are not taken, it may lead to critical under speed, causing the tripping of generators, cascading failures, and wide – area power blackouts. Tertiary control is applied to manage congestion, recover the secondary control reserve, and restore the frequency and tie line power to their fixed values when the secondary control reserve is insufficient. This service is frequently called manual frequency control and involves connecting and disconnecting power, relocating the output from frequency control participating units, and load demand side regulation.

In a conventional power system dominated by synchronous generators, the conceptual frequency response model, including four frequency control loops (i.e., primary, secondary, tertiary, and emergency controls) in a simplified structure, is shown in Figure 10. Frequency control loops are typically available. The market operator can balance the load generation of the system considering economy, reliability, and

resiliency. The operator can change the participation factors of the setpoint of all generators and power dispatch via secondary control and tertiary control. The operator can also perform generator tripping or load shedding in emergency situations.

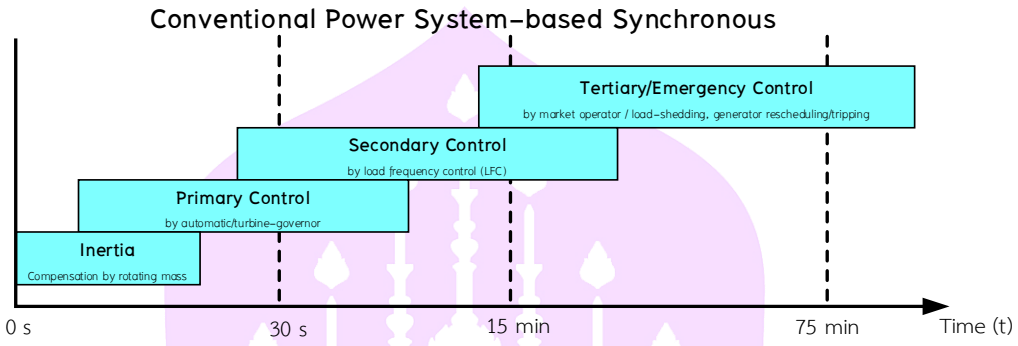


Figure 10 Timescale of frequency dynamic control for conventional power systems dominated by synchronous generators.

Source: Thongchart, et al., 2021, p. 15

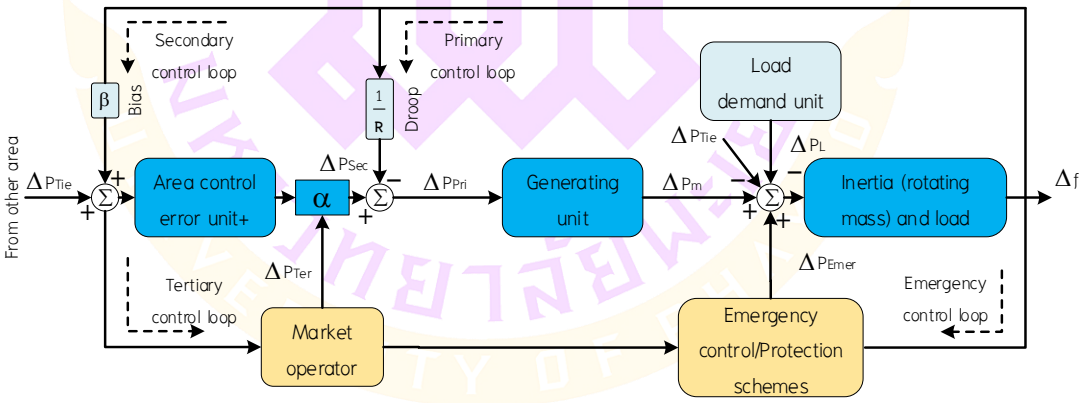


Figure 11 Conceptual frequency response structure with frequency control loops for a conventional synchronous generators – based power system.

In Figure 11, ΔP_m is the generated power change from a generating unit, ΔP_{Tie} is the change of interchanged power among areas, ΔP_L is the power change from load demand (as a disturbance), β is the area bias factor, R is the primary droop constant, α is the participation factor of a generating unit in frequency control, Δf is frequency deviation of the system, and ΔP_{Pri}, ΔP_{Sec}, ΔP_{Ter}, and ΔP_{Emer} are the control action signals for primary, secondary, tertiary, and emergency controls, respectively.

The grid frequency is regulated by the SG rotors, where the mechanical inertia and damping determine the frequency characteristics following the swing equation. To properly design the VIC and FDC of PV systems, the mechanism of the swing equation should first be investigated. Specifically, the swing equation is given as

$$\begin{cases} Pm - Pe = 2H\dot{\omega} + D(\omega - 1) \\ \theta = \omega - 1 \end{cases} \tag{12}$$

where

P_m and P_e is the mechanical power and the electromagnetic power of the SG,

H and D is the inertia constant and damping coefficient,

θ is the internal voltage phase angle of the SG.

All the variables here and thereafter are per – unit values.

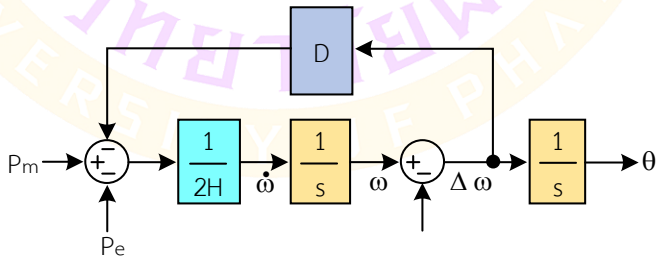


Figure 12 Diagram of the swing equation of the SG rotors, where $\Delta\omega$ indicates the frequency deviation.

The swing equation can be graphically represented as shown in Figure 12, where the inertia constant H and damping gain D determine the dynamics of the active power and frequency. Specifically, the inertia constant mainly determines the derivative of the frequency (i.e., the RoCoF), whereas the damping gain affects the frequency deviation more. In turn, in large – scale power systems, the RoCoF is highly dependent on the total inertia of the system, whereas the steady – state frequency deviation relies more on the total damping of the system. To further demonstrate the impacts of the inertia constant and damping gain on the frequency dynamics [39].

Inertia Power Compensation

In traditional power systems dominated by synchronous machines, the synchronous generators generate active power and kinetic energy, regulating the system frequency. The rotating mass in the rotor of a synchronous machine generates inertia power with the unit of Joule – seconds (J•s) or Watt – square second ($W•s^2$) for compensating the disturbances. The inertia power performs an important function in regulating the stability of the stable frequency of the system.

Inertia is generated when the rotating/spinning mass, rotor, or prime mover of a synchronous generator continues to spin unless it breaks down or stops. Subsequently, the majority of the inertia is contributed by the physical rotating mass related to the power outputs of the synchronous generators, enhancing the inertial response of the system. Thus, a minimum level of total system inertia is indispensable for solving two main dynamic issues. The first is to decrease the initial rate – of – change – of – frequency (RoCoF) after a large disturbance, preventing a cascading disconnection of the generators. The second is to arrest the frequency decay and limit the frequency nadir following a generation trip or load increment. In addition, inertia is used to arrest the frequency increase and reduce the frequency zenith following a load trip or a generation increment. The associated issues were investigated and reported in [17].

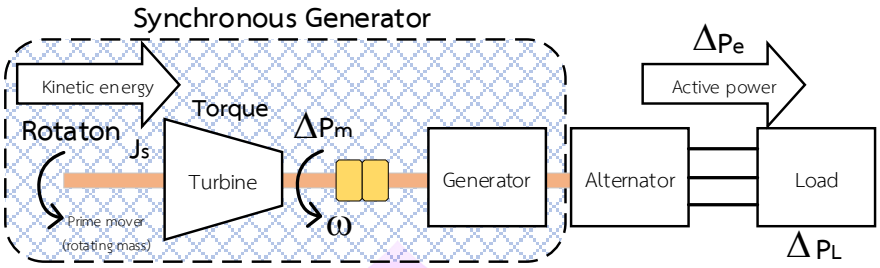


Figure 13 Schematic block diagram of a synchronous machine with respect to inertia power response.

Source: Thongchart, et al., 2021, p. 17

A schematic block diagram of a synchronous machine considering the dynamics of the inertia power response depicted in Figure 13 displays an overview of a typical 36 kVA synchronous generator equipped with an alternator manufactured by ABB at the Institute of Electrical Power Engineering and Energy Systems (IEE), Clausthal University of Technology, Germany. The alternator unit generates the frequency which is matched to the prime mover speed from the generator unit. Thus, the generator speed must be accurately and responsively controlled by the inertia power and speed governor (i.e., primary control) inside the generator unit to ensure the constant/stable frequency. A sudden increase in the load causes the generator and alternator units to slow down momentarily until the governor can adjust its speed. This momentarily reduces both the frequency and the voltage of the system. If the load suddenly reduces, the generator and alternator will speed – up momentarily before the governor can adjust its speed, causing both the frequency and voltage of the system to momentarily increase.

This section explains the dynamic model of frequency control, which pertains to inertia compensation and control, and how it is traditionally – based on the swing equation in synchronous machines as defined in [19].

$$J_s \frac{d\omega}{dt} = T_m - T_e = \frac{P_m}{\omega} - \frac{P_e}{\omega} \quad (13)$$

where

J_s is the moment of inertia with the unit of kg/m^2,

$\omega = 2\pi f_0$ is the angular velocity of the synchronous rotor (rad/s),

f_0 is the nominal frequency (Hz),

T_m and T_e are the mechanical and electrical torque for the generator,

P_m and P_e are the mechanical and electrical power for the generator (W).

In conventional power systems, there is often a disparity between the demand for electricity and its generation (ΔP). When this occurs, the kinetic energy ($E_{kinetic}$) stored in the rotating mass of a power generator is utilized to counteract the initial speed fluctuation. The frequency of the system is determined by the rotor speed of the generator. Consequently, any alterations in the rotor speed lead to changes in the system frequency, causing a deviation from the normal frequency value. The power generated by the generator in terms of kinetic energy can be represented using Equation (14).

$$\Delta P_{m\_inertia} = \frac{d}{dt} E_{kinetic} \quad (14)$$

Primary and Secondary Control

The power system frequency stability relies on the active power balance between the load and generation. The active power change at one point of a system affects the entire network by the deviation of the frequency. Thus, system frequency offers a useful index to signify an unbalance between system generation and load demand. Any short – term unbalance leads to an immediate variation in system frequency since the disturbance has been originally arrested by the inertia (kinetic) power of the rotor from 1 to 5 second. Significant loss of the generation without a suitable system control action creates severe frequency excursions outside the operating range of the power plant. Consequently, primary and secondary control schemes are required to avoid stability issues. These control schemes are the basic frequency control loops in power systems.

The power generated by a generator is determined by the mechanical power produced by its rotor or prime mover, such as a diesel engine, steam turbine, hydro – turbine, or gas – turbine. For hydro/steam turbines, the mechanical power is regulated by opening or closing valves, which control the flow of water or steam into the turbine. It is essential to continuously supply water or steam to the generators to match the actual power demand. A decrease in machine speed can cause a change in the frequency. To ensure the reliable operation of the power system, the system frequency should be maintained close to the nominal frequency of 50 or 60 Hz, depending on the system.

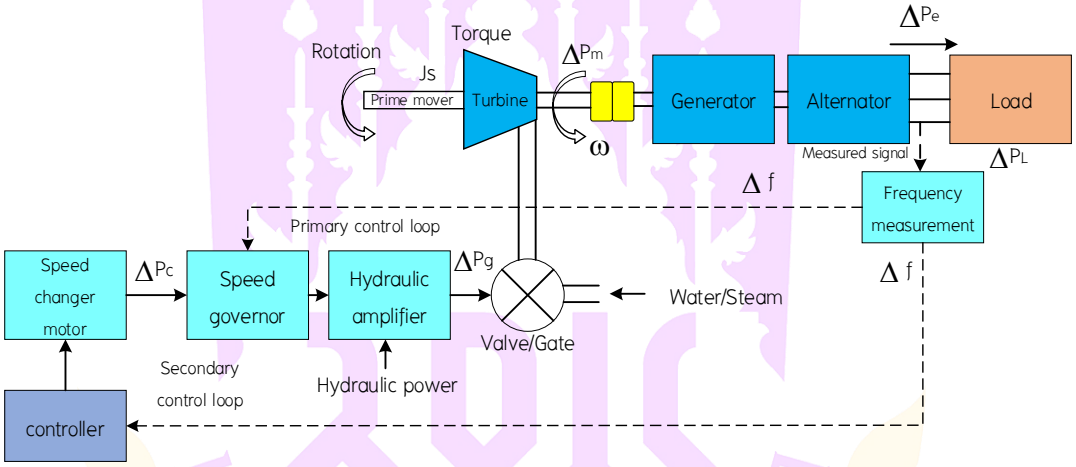


Figure 14 A schematic diagram of a synchronous generator with primary and secondary controls.

In terms of multiple operating generators, the primary control is equipped as a basic frequency control in all synchronous generators, while several large synchronous generators are provided with secondary control. A schematic diagram of a synchronous generator equipped with the primary and secondary controls is shown in Figure 14. The frequency experiences the transient deviation (Δf) after a load change (ΔP_L), the feedback mechanism automatically activates and provides a suitable control signal (ΔP_g) for the turbine unit to decrease or increase the mechanical power (ΔP_m) in a generation unit, tracking the load change and restoring the system frequency.

Table 2 shows the relation between power mismatch and frequency deviation. Generally, the frequency deviation indicates the power unbalance of the system and it should be regulated by using frequency control. Frequency control aims to balance the generated power and electrical demand to achieve a power system operation at the nominal system frequency. When the system frequency is higher than the nominal frequency due to over – generation ($P_m > P_e$ or P_L), to recover frequency back to its nominal value, the P_m must be reduced to achieve the balance with the P_e or P_L. On the contrary, when the frequency of the system is lower than the nominal frequency due to lack of generated power ($P_m < P_e$ or P_L), the Pm must be increased to achieve the balance with the P_e or P_L and restoring frequency to its nominal value.

Table 2 Relationship between power mismatch and frequency deviation.

Power mismatch	Rotor speed (df / dt or $d\omega / dt$)	Frequency deviation (Δf)
$P_m > P_L$	Plus (acceleration)	Increasing
$P_m = P_L$	Zero (no acceleration)	Stable
$P_m < P_L$	Minus (deceleration)	Decreasing

The relation between mechanical power and electrical power can be represented by the swing equation in Equations (15) – (16).

$$P_m - P_e = M\frac{df}{dt} + D\Delta f \qquad (15)$$

$$M = 2H(\text{in per} - \text{unit}) \text{ or } M = 2H / f_0 \qquad (16)$$

where

M is the moment of inertia with the unit of J_s or $W \cdot s^2$,

H is the inertia constant, presented in a unit of second,

f_0 is the nominal frequency.

In addition to the primary control, the speed governor measures the variation in speed (i.e., frequency) through the loops of the primary and secondary controls. The hydraulic amplifier offers the required mechanical forces to adjust the primary valve against the high pressure from water or steam. The speed changer delivers a steady – state power output setting for the turbine.

At each generating unit, the speed governor delivers the primary speed control function, with all the generating units contribute to the frequency regulation without considering the locations of load variation. However, the primary control is not usually efficient to recover the frequency of the system, particularly in an interconnected system. Thus, the secondary control loop equipped in a large synchronous generator is applied to correct the load reference setpoint via the speed changer motor. The secondary control loop provides feedback on the measurement of frequency deviation via a dynamic controller. In real practice, a simple integral (I) or proportional – integral (PI) controller is used as a dynamic controller. The output signal (P_c) was then used to maintain the system frequency.

Structure of Frequency Response Model

The dynamic characteristic of the power system is usually time varying and nonlinear. However, to perform frequency control synthesis with respect to variation in load or output power of RESs, a linearized low order structure is used. The dynamic effects of the frequency response are quite slow compared with the rotor angle and voltage dynamics on the timescale of seconds to minutes.

Moreover, to perform the analysis of slow and fast power system dynamics by analyzing the dynamics of generation and load in detail, complex numerical techniques are required to allow changes in the simulation time step with the amount of fluctuation in the system parameters. By ignoring the fast dynamics of the rotor angle and voltage, the complexity of the computation, data requirements, and modeling can be reduced. Therefore, the results and analysis were simplified.

A simplified structure of the frequency response for the schematic diagram in Figure 15, considering one generating unit, is explained in this section.

The whole generator – load dynamic relation between the incremental mismatch power ($\Delta P_m - \Delta P_L$) and frequency deviation (Δf) using Equation (17).

$$\Delta P_m(t) - \Delta P_L(t) = 2H\frac{d\Delta f(t)}{dt} + D\Delta f(t) \qquad (17)$$

where

H is the inertia constant,

D is the load damping coefficient.

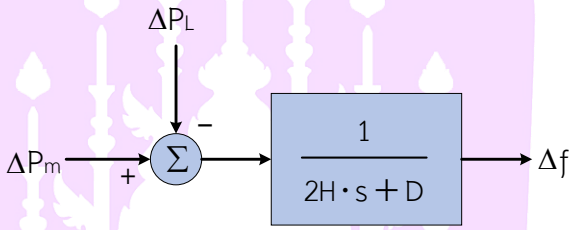


Figure 15 Block diagram of the load generator model for frequency control study.

The load damping coefficient is directly determined as a percent variation in load for 1% variation in frequency. For example, a specified value of 2 for D indicates that a 1% variation in frequency could result in a 2% variation in load. Equation (17) is then transformed into a Laplace term using (18).

$$\Delta P_m(s) - \Delta P_L(s) = 2Hs\Delta f(s) + D\Delta f(s) \qquad (18)$$

where

ΔP_c is the change (signal) of secondary control action,

ΔP_g is the change (signal) of governor control action.

Equation (18) can be represented as a block diagram, which significantly reduces the complexity of the schematic block diagram of the closed loop synchronous generator model in Figure 16 [40]. The frequency response of a system relies on the integrated effects of the control droops of the speed governors (generators) and loads.

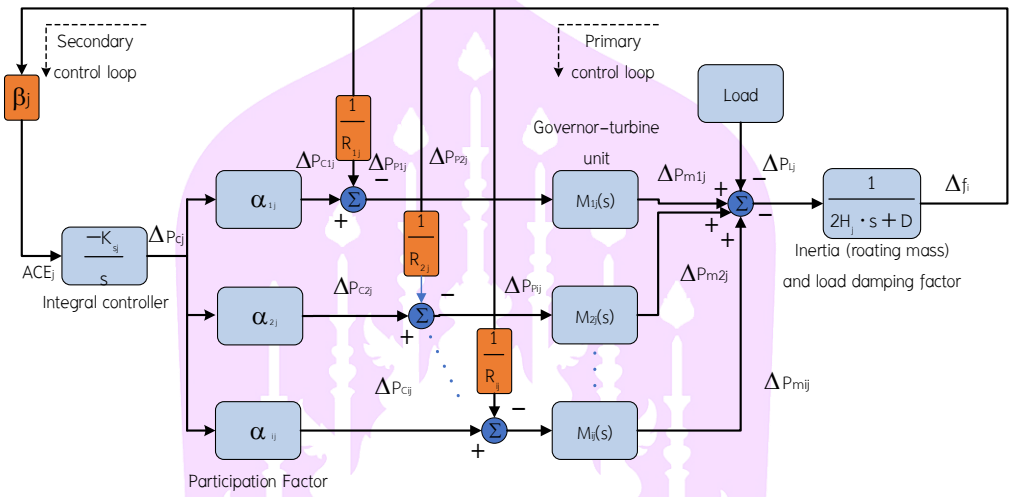


Figure 16 Frequency response model of a single – area system with multiple generators.

$$\Delta f_{ss} = \frac{-\Delta P_L}{\left(\frac{1}{R_1}+\frac{1}{R_2}+\cdots+\frac{1}{R_i}\right)+D} = -\frac{\Delta P_L}{\left(\frac{1}{R_T}+D\right)} \tag{19}$$

$$R_T = \frac{1}{\frac{1}{R_1}+\frac{1}{R_2}+\cdots+\frac{1}{R_i}} \tag{20}$$

where

R_i is the droop characteristic at the generator I,

R_T is the equivalent droop characteristic.

Frequency Regulation in a Single – Area Power System

To perform frequency stability study and analysis for a single – area power system, it is common to model a multi generator dynamic behavior using an equivalent generator model, as displayed in Figure 17. Subsequently, the combined model in Figure 17 can be used as an equivalent frequency analysis model for all generators of a one – area power system.

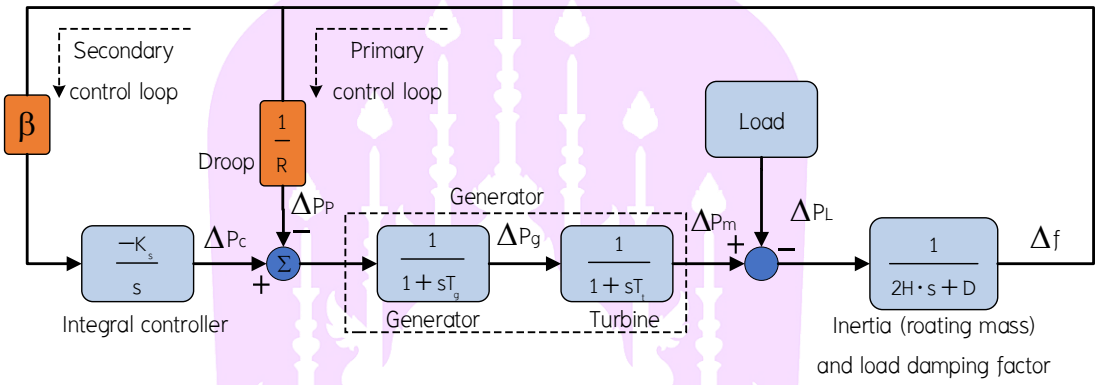


Figure 17 Combined dynamic model of a non – reheat steam generator with inertia compensation, primary and secondary controls for frequency analysis.

Source: Thongchart, et al., 2021, p. 30

In addition to the system loads and generators, the equivalent model combines the damping effects into a single damping factor/constant. The equivalent system inertia constant is assumed to be equal to the sum of the inertia constants of all generating units. Nevertheless, the generator turbines and individual control loops have similar control parameters and response behaviors. It should also be noted that the equivalent structure is useful only for simplifying the frequency stability study and analysis of an isolated system.

Table 3 Simulated parameters for the isolated system.

Parameter	Value
Gain of integral controller, K_s(s)	0.35
Governor time constant,T_g(s)	0.07
Turbine time constant,T_t(s)	0.37
Governor droop constant,R(H_z/p.u.)	2.60
Bias factor, β (p.u. s)	0.98
System inertia constant,H(p.u. s)	0.083
System load damping coefficient,D(p.u./H_z)	0.016

The dynamic response of the single – area power system due to sudden (step) changes of the load disturbance (0.02 p.u. at 3 s and 0.01 p.u. at 15 s) is plotted in Figure 17. This figure shows the importance of the primary and secondary control deployments during disturbances. By applying only primary control, it is obvious that the frequency of the system cannot be restored to its nominal value. By integrating the secondary control into the system, the system frequency can properly restore its nominal value within a few seconds. Evidently, the frequency nadir and overshoot of the system significantly reduce. The system parameters for the conducted simulation are shown in Table 3. The simulation is performed using the MATLAB/Simulink environment [40]. To investigate the effect of inertia power compensation, the system inertia constant was reduced by 50% from its nominal value and dynamic response. Due to the reduction of inertia power, it is obvious that the inertial response of the system consequently reduces, resulting in higher RoCoF. Consequently, it yields a larger frequency overshoot and nadir, which requires a longer stabilizing time after the disturbance. Moreover, following the disturbance, the generated power fluctuated more, leading to stress in the generating unit.

Analysis of Steady – State Frequency Response

To perform the frequency response analysis, it is assumed that all generator units i in a control area j are non – reheat steam systems and are represented by Equation (21).

$$M_{ij}(s) = \left[\frac{1}{1+sT_{gij}}\right] \cdot \left[\frac{1}{1+sT_{tij}}\right] \tag{21}$$

Then, the frequency deviation in area j can be obtained using Equation (22).

$$\Delta f_j(s) = \frac{1}{2H_j + D_j}\left[\sum_{i=1}^{n} \Delta P_{mij}(s) - \Delta P_{Lj}(s) - \Delta P_{Tie,j}(s)\right] \tag{22}$$

where

$$\Delta P_{mij}(s) = M_{ij}(s) \cdot \left[\Delta P_{Cij}(s) - \Delta P_{Pij}(s)\right] \tag{23}$$

To examine the effect of inertia power compensation, the system inertia constants for all areas were reduced by 50% from their nominal values and dynamic response. Due to the reduction of inertia power, it is obvious that the inertial response of all areas consequently reduces, resulting in higher RoCoF and larger frequency overshoot and nadir, with longer stabilizing time after the disturbances. Moreover, following the disturbance, the generated power in all areas is more fluctuating, leading to the stress in all generating units.

$$\Delta P_{Pij}(s) = \frac{\Delta f_j(s)}{R_{ij}} \tag{24}$$

In the equations above, ΔP_P is the change (signal) in primary control action, ΔP_C is the change (signal) in secondary control action, and ΔP_{Tie} is the tie – line power change for an interconnected power system. In a single – area power system, $\Delta P_{Tie} = 0$. The α_{ij} is the frequency control participation factor in the control area j f_o the generator unit i, which will be explained in the following section.

Substituting Equations (23 – 24) into Equation (22) the resulting equation can be represented as Equation (25).

$$\Delta f_j(s) = \frac{1}{2H_j + D_j}\left[M_{ij}(s) \cdot \left[\Delta P_{Cij}(s) - \frac{\Delta f_i(s)}{R_{ij}} \right] - \Delta P_{Lj}(s) - \Delta P_{Tie,j}(s) \right] \quad (25)$$

For load disturbance analysis, ΔP_L is considered as a step function in Equation (26).

$$\Delta P_{Lj}(s) = \frac{\Delta P_{Lj}}{s} \quad (26)$$

Substituting Equations (25 – 26) the resulting equation can be summarized as Equation (27).

$$\Delta f_j(s) = \frac{1}{L_j(s)}\left[M_{ij}(s) \cdot \Delta P_{Cij}(s) - \Delta P_{Tie,j}(s) \right] - \frac{\Delta P_{Lj}}{sL_j(s)} \quad (27)$$

where

$$L_j(s) = 2H_j + D_j + \frac{M_{ij}(s)}{R_{ij}} \quad (28)$$

By substituting Equation (21) into Equations (27 – 28) and applying the final value theory, the steady – state frequency deviation of the system can be obtained using Equation (29).

$$\Delta f_{ss,j} = \lim_{s \to 0} \Delta f_j(s) = \frac{1}{L_j(0)}\left(\Delta P_{Cij} - \Delta P_{Lj} \right) \quad (29)$$

Assuming that ΔP_{Tie} is equal to zero at the steady – state, thus Equation (30) – (31).

$$\Delta P_{Cj} = \lim_{s \to 0} \left(\sum_{i=1}^{n} M_{ij}(s) \cdot \Delta P_j(s) \right) \tag{30}$$

$$L_j(0) = \sum_{i=1}^{n} \frac{1}{R_{ij}} + D_j = \frac{1}{R_{Tj}} + D_j \tag{31}$$

where

R_{Tj} is the equivalent droop characteristic for area j and is represented.

$$\frac{1}{R_{Tj}} = \sum_{i=1}^{n} \frac{1}{R_{ij}} \tag{32}$$

Based on Equation(20), $L_j(0)$ is equivalent to the frequency response characteristic of the system (β_j) using Equation (33).

$$\beta_j = \frac{1}{R_{Tj}} + D_j \tag{33}$$

By applying Equations (29), (31), can be rewritten as Equation (34).

$$\Delta f_{ss,j} = \frac{\Delta P_{Cj} - \Delta P_{Li}}{1/R_{Tj} + \Delta D_j} \tag{34}$$

From Equation (34), it can be seen that if the magnitude of the disturbance matches with the available power reserve via secondary control ($\Delta P_{Cj} = \Delta P_{Li}$), the system frequency deviation becomes zero at the steady – state condition. For large generating units, a suitable R_{ij} is between 0.05 and 0.1.

In the case of a small value of D_j and R_{Tj}, Equation (34) can be reduced using Equation (35).

$$\Delta f_{ss,j} = \frac{\left(\Delta P_{Cj} - \Delta P_{Li}\right)R_{Tj}}{R_{Tj}D_j + 1} \cong \left(\Delta P_{Cj} - \Delta P_{Li}\right)R_{Tj} \tag{35}$$

In the case of no secondary control ($\Delta P_{Cj} = 0$), the frequency deviation in steady – state depends on the magnitude of the disturbance using Equation (36).

$$\Delta f_{ss,j} = \frac{\left(-\Delta P_{Li}\right)R_{Tj}}{R_{Tj}D_j + 1} \tag{36}$$

To simplify the dynamic frequency analysis, the governor turbine time constants were considered to be smaller than the time constant of a power system (rotating mass and load). Thus, it is acceptable to assume that T_{gi} and T_{tj} are zero. Under this condition, Equation (27) can be reduced using Equation (37).

$$\Delta f_j(s) \cong -\frac{\Delta P_{Lj}}{s}\left(\frac{1}{2H_j + D + \frac{1}{R_{Tj}}}\right) \tag{37}$$

By simplifying Equation (37) and arranging it into partial fractions, the resulting equation can be represented using Equation (38).

$$\Delta f_j(s) \cong \frac{\left(-\Delta P_{Lj}\right)R_{Tj}}{R_{Tj}D_j + 1}\left(\frac{1}{s} + \frac{1}{s + \frac{R_{Tj}D_j + 1}{2H_jR_{Tj}}}\right) \tag{38}$$

By substituting Equations (36) – (38), the resulting equation can be represented as Equation (39).

$$\Delta f_j(s) \cong \Delta f_{ss,j}\left(\frac{1}{s} - \frac{1}{s+\tau_j}\right) \tag{39}$$

where

τ_j is the time constant of the closed – loop system represented as:

$$\tau_j = \frac{1+R_{Tj}D_j}{2H_jR_{Tj}} \tag{40}$$

By applying the inverse Laplace transformation to Equation (39), the equation can be rewritten in terms of the time domain by using Equation (41).

$$\Delta f_j(t) \cong \Delta f_{ss,j}\left(1-e^{-\tau_j(t)}\right) \tag{41}$$

The AC Microgrids

A microgrid is a localized group of electricity sources and loads that are normally connected to and synchronous with the traditional large – scale power grid (microgrids). But can also disconnect to "island mode" and function autonomously as physical or economic conditions dictate. Microgrids can be powered by a variety of sources including solar, wind, and fossil fuels. They are often used in remote, rural, or urban areas to improve the reliability and resilience of the overall power system [41].

Where the energy sources are connected through a low – voltage distribution network coupled with the electrical loads. In this structure, the sources and loads are placed close to each other, and for the smooth operation of the microgrids, the storage devices are also connected in the system. The system configuration of the AC Microgrids investigated in this study is shown in Figure 18. It consists of a wind turbine generator (WTG), diesel engine generator (DEG), fuel cell (FC), photovoltaic system (PV), battery energy storage system (BESS), and flywheel energy storage system (FESS). Mathematical models consist of the first – order transfer functions of the subsystems that constitute the system.

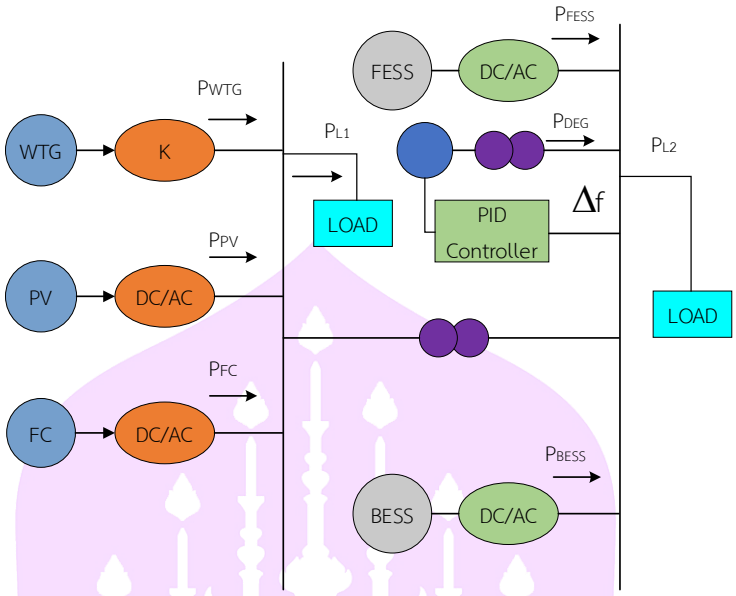


Figure 18 Configuration of AC Microgrids Investigated.

The total power generated (Ps) of the AC Microgrid is the total of all the output powers of the power of WTG (PWTG), DC – AC converter connected to FC (PFC), PV (PPV), exchanged power of BESS (PBESS), power of FESS (PFESS), and output power of DEG (PDEG). P_S was determined using Equation (42).

$$P_S = P_{WTG} + P_{PV} + P_{FC} + P_{DEG} \pm P_{FESS} \pm P_{BESS} \quad (42)$$

Table 4 Parameter values.

Rated Power (KW)		Load (KW)	
WTG	125	P_{L1}	220
PV	25		
FC	70		
DEG	150	P_{L2}	200
FESS	40		
BESS	40		

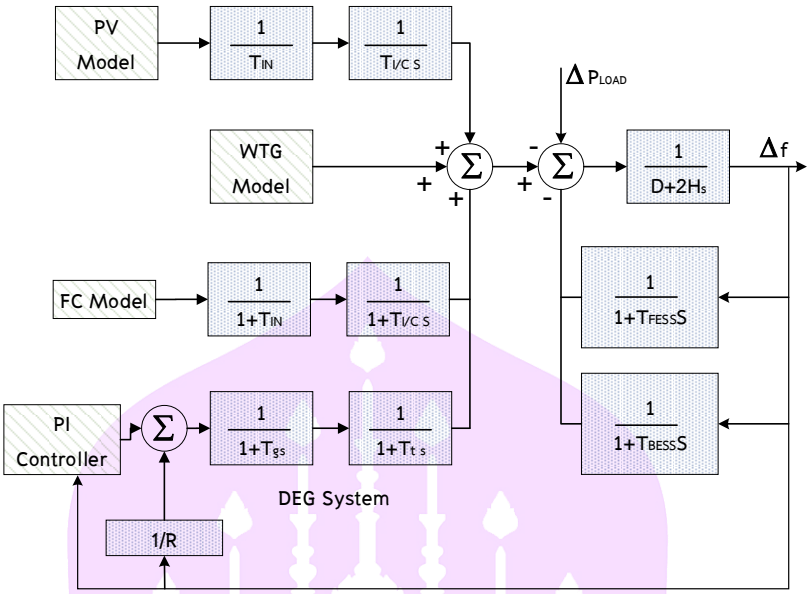


Figure 19 Block diagram representation of frequency Response model of an AC microgrid.

Source: Amandeep and Sathans, 2016, p. 3

Table 5 AC Microgrid Parameter Values.

Parameter	Values
D (p.u./Hz)	0.015
H (p.u./s)	0.1667
T_{FESS} (s)	0.1
T_{BESS} (s)	0.1
R (Hz/p.u.)	3
T_g (s)	0.08
T_t (s)	0.4
$T_{I/C}$ (s)	0.004
T_{IN} (s)	0.04

The ratings of the DG units and loads adapted from literature are listed in Table 4. For frequency regulation, the DEG functions as a spinning reserve with a small amount of power. A block diagram representation of the frequency response model of the AC Microgrid is shown in Figure 19, and the parameter values are listed in Table 5.

Cyber Attacks

The local controller requires the state information of its neighborhood to assist in regulating local system dynamics. Because the state transmission process depends on open communication networks, which exposes the multi – area power system to cyberattacks, it is presumed that adversaries are familiar with the system's interaction topology and can arbitrarily launch cyberattacks – based on their particular attempts. Before the state information is transmitted from the neighboring control centers to the locals, adversaries may filch the default code in some ways to enter the data sending unit and falsify the measurements of states. During the transmission process, they may tamper with the communication protocols of the vulnerable networks. Both attacks ruin the true values of the state measurements and degrade the system dynamics of all areas [42].

From the perspective of adversaries, any category of cyberattacks (e.g., denial of service (DoS) attacks and false data injection (FDI) attacks) can be initiated. FDI attacks show more powerful attacking capability, which can corrupt the transmission in any tricky form, and cyberattacks on the state transmission process (open communication links) as FDI attacks. The practical received state measurement of area i transmitted from area j under FDI attacks is depicted using Equation (43).

$$\tilde{y}_j(k) = y_j(k) + G_j g_j(k) \tag{43}$$

where

$y_j(k)$ is the true measurement from sensors of area j,

$G_j g_j(k)$ indicates malicious data injected into the open communication links.

Cyber Attacks Scenarios

Remark 1: The field sensors are susceptible to cyber intrusions, and an attacker can easily hack into sensors that perform local machine speed measurements. Nevertheless, one machine speed measurement is processed through the private channel, which is deemed to be invulnerable to attacks by a sufficiently high level of security. Remark 1 explains the situation (position) in which the attacker can implement attacks. Remark 1 is understandable and pragmatic in that field sensors for machine speed measurement are the most critical elements for frequency destabilization, whether in a distributed or centralized control mode, and the rudimentary protection measures of sensors are likely to be considered for this type of attacks, which can be easily penetrated.

Remark 2: The reference value for distributed control (tracking) in this study is assumed to be vulnerable to cyber intrusion, which means that the attacker can infiltrate the distributed system and falsify the reference value. Remark 2 further pushes the boundary of attacks scenarios into a control parameter (reference value) distortion – based on the misrepresentation of the feedback state information. It must be noted that the control parameter is another important element for guaranteeing the success of controller execution. It has become a natural and primary target of cyberattacks.

Robust and Resilient Distributed Optimal Frequency Control

To make the distributed optimal frequency control robust against cyberattacks, a set of auxiliary agents (AAs) corresponding to each of the control agents (CAs) is introduced. The state vector of these AAs is denoted as $Z = \left[Z_1 \ldots, Z_n\right]^T$, which are cyber states with no physical meaning designed to maintain stability of the overall system in the presence of cyberattacks.

The CAs and AAs are interconnected by another layer of communication network, which is denoted as auxiliary network $\sum_h$. The fast – growing 5G communication, which enjoys merits of low – latency and cost – effectiveness, provides an ideal platform to implement the proposed distributive controlled cyber – physical MGs, network slicing approach has been developed to partition one shared physical infrastructure into multiple

virtual networks. The configurations among various slices, such as security functions, are independent and do not affect each other. Therefore, it is possible to confine the impact of security requirements to a single slice, rather than to the whole network. When the control network Σ_s and auxiliary network Σ_h of the proposed robust and resilient distributed control are implemented in two isolated slices. Assumption 1, as presented below, can be satisfied with a very high possibility. Meanwhile, facilitated by software – defined networking approach, the topologies of 5G communication slices Σ_s and Σ_h can be flexibly programmed. Specifically, it is required that the communication topology of Σ_h is designed to be the same as Σ_s, i.e., CA(AA) j can communication to AA (CA) i if and only if $(i, j) \in \varepsilon_s$ in Σ_s, as illustrated by Figure 20.

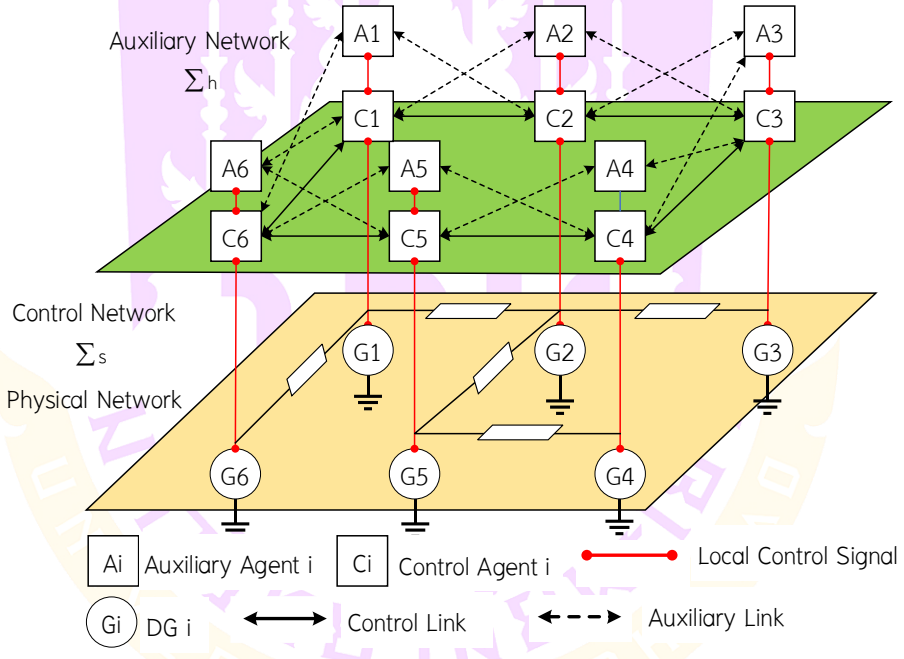


Figure 20 Illustrative diagram of the cyber – physical MG and the communication architecture.

Source: Liu, et al., 202, p. 379

Assumption 1: The control network Σ_s and the auxiliary network Σ_h cannot be compromised simultaneously. Based on the cyber – physical infrastructure, the overall dynamics of interconnected CAs and AAs can be engineered using Equation (44).

$$\text{CAs} = -L_\theta + \beta K_s z - k_I \Delta\omega\_ \in_\theta \tag{44}$$

$$\dot{z} = -H_z + \beta G\theta - \beta k_I \Delta\omega + \in_z \tag{45}$$

where

CAs	is the dynamics of the CAs.
L	is the Lagrangian matrix that interlinks the CAs.
θ	is $[\theta_1,...,\theta_n]^T$
k_I	is $[k_{I1},...,k_{In}]^T$
β	represents a sufficiently large control gain.
K_s	is the interconnection matrix between the AAs and CAs.
z	is the virtual state.
H_z	is local feedback matrix of AAs.
G	is the interconnection matrix between the CAs and AAs.
$\in_\theta$ and $\in_z$	is FDI attacks imposing on CAs/AAs.

The control parameters required using Equation (44) – (45) can be designed according to the following steps.

Step 1: A sufficiently large: $\beta > 0$ should be agreed upon by all the CAs and AAs.

Step 2: Local Feedback Parameters: For the CAs and AAs, local feedback of the frequency deviation is required with a gain vector $k_I = \frac{K_1}{\alpha^T 1}\alpha$, where K_1 is a positive control gain and $\alpha = \frac{\rho}{k_P^T 1}$ is based on the participation factor vector $\rho = [\rho_1,\ldots,\rho_n]^T$ and droop gain vector $k_P = [k_{P1},\ldots,k_{Pn}]^T$. The AAs do not require any mutual

communication but just local feedback, which indicates that H is selected as a diagonal matrix as $H = -K_2 I$ with $K_2 > 0$.

Step 3: Control Network Slice Σ_s : The communication matrix *L* can be selected as any sparse matrix according to the communication topology of Σ_s. Thus, the communication overhead required by Σ_s is the same as the conventional approach, i.e., N_c messages are distributivity transmitted at each time instant.

Step 4: Auxiliary Network Slice Σ_h : For communication from CAs to AAs, the interconnection matrix is G = L, and, thus, N_c messages are required to be communicated at each time instant. For communications from AAs to CAs, the interconnection matrix can be designed as $K_s = -L - K_1 \mathrm{diag}(\alpha)$, which has the same structure as L, and thus the required communication overhead is also N_c messages per time instant. Therefore, we conclude that Σ_s and Σ_h share the same communication topology, and the communication overhead of Σ_h is twice of that required by Σ_s.

Attack – resilient control can adopt the same distributed communication topology at the cost of a trebling communication overhead. It should be noted that the communication burden can be further alleviated by adopting the event – triggered mechanism. During typical operation, AAs can be inactive until a specific alarm is triggered [43].

Model Predictive Control

Model Predictive Control (MPC) is a feedback control scheme that generates control action – based on the open – loop optimization method over a finite horizon with the measured state as the initial state. In addition to being intuitively attractive (choosing an action – based on its impact in the future rather than just reacting to the present), MPC also offers the possibility of incorporating control and state constraints that few feedback control methods can claim. Stability is an important issue in the MPC algorithm. To guarantee the stability of the MPC algorithm, various constraints have been used. They include the terminal equality constraint, terminal inequality constraint, terminal cost, and a combination of the terminal cost and constraint. In our study present

a state – contractive constraint – based MPC scheme guarantees the stability of the MPC algorithm by introducing a state – contractive constraint [44]. To describe the algorithm, we considered a discrete nonlinear system using Equation (46).

$$x(k+1) = f(x(k)) + g(x(k))u(k) \tag{46}$$

where

$x \in R^n$ The state variable

$u \in R^m$ The control variable

$k = 1,2,\ldots$ The optimization problem at control step k $(k = 1,2,\ldots)$

$$\min J(x, \underline{u}) \tag{47}$$

$$\underline{u}(k) = \{u(k|0), u(k|1), \cdots, u(k|M-1)\} \tag{48}$$

subject to :

$$x(k|i) = f(x(k|i-1)) + g(x(k|i-1))u(k|i-1) \tag{49}$$
$$i = 1,2,\cdots,M$$

$$x(k|0) = x(k) \tag{50}$$

$$\underline{u}(\cdot) \in U \tag{51}$$

$$\left\|x(k|1)\right\|_2 \le \rho \left\|x(k-1|1)\right\|_2 \text{ and } \left\|x(0|1)\right\|_2 \le \left\|x(0)\right\|_2 \tag{52}$$
$$\rho \in [0,1)$$

where

M is the length of the predictive horizon.

The optimal control sequence at control step k using Equation (53).

$$\underline{u}^{\circ}(k) = \left\{u^{\circ}(k|0), u^{\circ}(k|1), \cdots, u^{\circ}(k|M-1)\right\} \tag{53}$$

The optimal state trajectory at the control step k corresponds to the optimal control sequence in Equation (53) using Equation (54).

$$x^{\circ}(k) = \left\{x(k|1), x(k|2), \cdots, x(k|M)\right\} \tag{54}$$

where

$J(x,u)$	The objective function
$u^{\circ}(k\|i-1)(i=1,\ldots M)$	The i predictive control signal in $u^{\circ}(k)$
$x(k\|i)$	The i predictive state in $x^{\circ}(k)$
$x(0)$	The initial state of the system
$x(k)$	The observed state at control step k

The inequality constraint in Equation (52) is the state – contractive constraint. The contractive constraint is updated at every control step. In other words, the system state will be contracted at every control step. $\rho \in [0,1)$ is the contractive parameter. The control algorithm at control steps k.

Data: $x(0), M, \rho \in [0,1), T$ (sampling time),

Step 1: Set $k = 0$,

Step 2: Solve SCC – MPC problem, result is the optimal control sequence using Equation (53),

Step 3: $u(k) = u\circ(k|0)$ to the system,

Step 4: Update the necessary information for the next control step, such as the state – contractive constraint. Set $k = k+1$, turn to steps 2.

In Step 2 we assume that the control problem is feasible for all k, (k=1,2, ...). This means that there always exists a solution that satisfies all constraints and renders the objective function finite. Without loss of generality, we assume that $x^{*}, u^{*} = (0,0)$ is the equilibrium point of system.

MPC Method

The MPC method is based on current measurements and predictions of future output values [45]. The objective of MPC is to determine a sequence of control moves, that is, the manipulated input variable, so that the predicted response moves to the set point in an optimal manner. Figure 21 shows the basic concept of the MPC.

calculates a set of M values of the input $\{u(k+i-1), i=1,2,3,...,M\}$. The set consists of the current input u(k) and M – 1 future inputs. The input is held constant after M controls move. The inputs are calculated so that a set of P predicted outputs $\{\tilde{y}(k+i), i=1,2,...,P\}$ reaches the set point in an optimal manner.

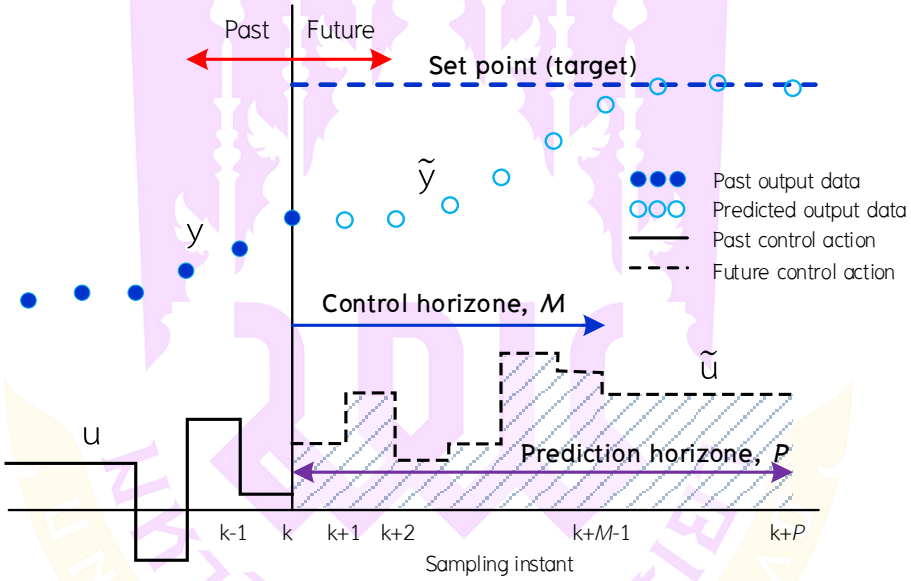


Figure 21 Basic concept of MPC.

Source: Jonglak and Issarachai, 2016, p. 99

where

y	is the actual output,
$\tilde{y}$	is the predicted output,
u	is the manipulated input,
k	is the current sampling instant.

The prediction horizon, denoted by the variable P, represents the number of forecasts made, whereas the control horizon, denoted by the variable M, represents the number of control moves executed. Although a series of M control moves is computed at each sampling point in time, only the first move is performed. Following the availability of new measurements, a fresh sequence of control moves was calculated at the subsequent sampling point in time; however, only the initial input move was implemented. This process was repeated at each sampling instant.

The MPC predictions are made using a dynamic model, typically a linear empirical model such as a multivariable version of the step response or difference equation models. Alternatively, a transfer function or state – space model can be employed.

The MPC technique resolves an optimization problem for a finite number of future time steps at the present moment. Consequently, the system can be represented by its finite impulse response using Equation (55).

$$y(k+1) = y(k) + A\sum_{i=0}^{n_T} \delta_i u(k-i) \tag{55}$$

where

$y(k)$ is the vector of manipulated moves at time instance (k),

$u(k)$ is the input at time instance (k),

n_T is number of impulse response coefficients used modeling system,

A is the interaction matrix,

δi is the coefficient number and can be defined using Equation (56).

$$\delta_i = g_{i+1} - g_i, \quad \forall_i = 0,\ldots,n_T \tag{56}$$

where

g_i is the scalar,

g_iA is the i_{th} impulse response coefficient matrix.

The MPC problem involves computing u(k) as solution quadratic program (QP).

$$\min_{u(k)\in M} \sum_{j=1}^{M} [y(k+j) - r(k+j)]^{T} W_y [y(k+j) - r(k+j)] + [u(k) - u(k-1)]^{T} W_u [u(k) - u(k-1)] \quad (57)$$

Subject to $$y(k+1) = y(k) + A \sum_{i=0}^{n_T} \delta i u(k-i)$$

$$-\Delta u_{max} + u(k-1) \le u(k) \le \Delta u_{max} + u(k-1)$$

where

$r(k+j)$ is the desired profile,

W_y and W_u are positive semidefinite weighting matrices,

M is the control horizon.

Each weight (W_y, W_u) is assumed to be a constant multiplied by the identity matrix, which is appropriate for WTG blade pitch angle and PHEV control. In particular, W_u is often selected as sufficiently large that the rate constraints are satisfied [46].

MPC – Based VESS for Virtual Inertia and Frequency Regulation

The proposed MPC – based VESS for virtual inertia and frequency regulation [47] is shown at the bottom of Figure 22. The VESS controller consists of two loops: the MPC1 – based indoor temperature and microgrid frequency regulation control loop and the MPC2 – based virtual inertia (or RoCoF) control.

In the initial iteration, the Model Predictive Control 1 (MPC1) simultaneously regulates the indoor temperature to a predefined reference value and minimizes the power system frequency deviation. MPC1 takes into account both indoor temperature and frequency deviations as its inputs, which are then appropriately weighted. The objective of the weighting process was to maintain a comfortable indoor temperature while maintaining the frequency deviations within acceptable limits. Meanwhile, in the second loop, MPC2 forecasts the inertial gain of the virtual inertia emulator. The predicted inertial gain is used to produce the RoCoF control signal. Thus, MPC2 regulates RoCoF deviation (ΔRoCoF) to the reference value ($\Delta RoCoF_{ref}$) Finally, the control signals from the MPC1 and MPC2 loops were summed to obtain the control signal for regulating VESS power.

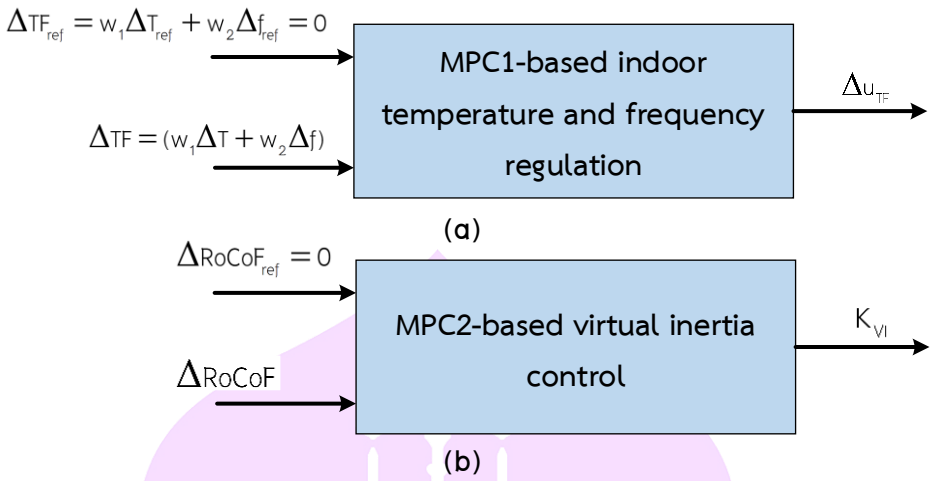


Figure 22 Concept of MPC – based VESS control (a) MPC1 (b) MPC2.

In addition, the power consumption of IACs may peak during daylight hours. To prevent excessive consumption and reduce high frequency deviation during emergencies, IACs cannot consume more power. The regulation of PV power generation through maximum power point tracking is employed to assist IACs in supporting the virtual inertia emulator.

Inverter air conditioning (IAC) systems can be utilized for frequency regulation by adjusting parameters K_1 and K_2. These parameters can be replaced by controllers such as proportional – integral (PI) and model predictive control (MPC) controllers. However, studies have shown that MPC controllers are more effective than PI controllers in regulating indoor temperature and frequency deviations. Therefore, in this study, the power consumption of the IAC was controlled by MPC controllers to regulate indoor temperature and frequency deviations.

The MPC1 – based indoor temperature and frequency controls are shown in Figure 22 (a). The feedback control signal Δ_{uTF}, calculated using MPC1, was employed to control indoor temperature and frequency deviation. The input of MPC1 was the summation of the weighted indoor temperature deviation $W_1\Delta T$ and the weighted frequency deviation $W_2\Delta f$. The selection of indoor temperature weight w_1 and frequency weight w_2 is important because temperature deviation ΔT and frequency deviation Δf are affected by indoor temperature weight w_1 and frequency weight w_2, respectively.

Figure 22 (b) shows MPC2 – based virtual inertia control. The inputs and outputs of MPC2 are the rate of change of the frequency deviation ΔRoCoF and initial gain of the VESS (K_{v1}), respectively.

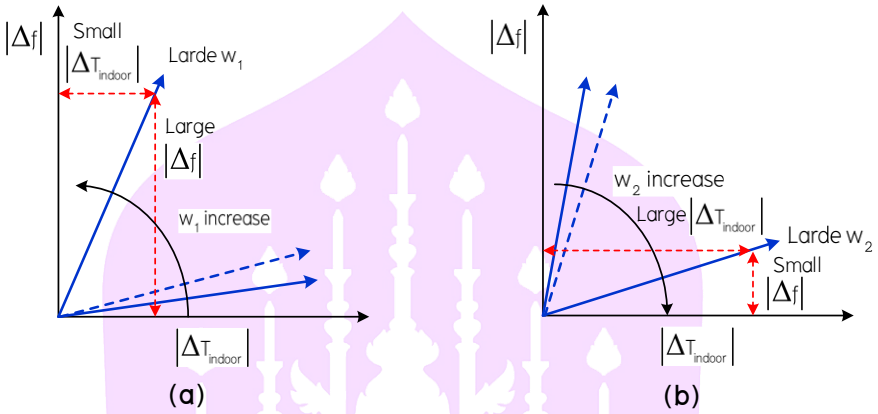


Figure 23 Impact of MPC1 is input (a) weights to w_1 and (b) impact of w_2.

Figure 23 illustrates the effect of MPC1's input weights (w_1 and w_2) on the absolute indoor temperature deviation. $|T_{indoor}|$ and absolute frequency deviation $|\Delta f|$. For explanatory purposes, this section uses w_1 and w_2 instead of K_1 and K_2, respectively. In addition, T_{indoor} and Δf is changed to $|T_{indoor}|$ and $|\Delta f|$, respectively. Therefore, can be rewritten as Equation (58).

$$\Delta f_{IAC} = w_1 |\Delta T_{indoor}| + w_2 |\Delta f| \quad (58)$$

When w_1 increases (w_2 = constant), $W_1\Delta T$ increases and is minimized by the MPC1 procedure. Therefore, the indoor temperature deviation ΔT reduced more than the frequency deviation Δf. The red dotted lines indicate that a large indoor temperature weight W_1 produces a small indoor temperature deviation ΔT and large frequency deviation Δf. When the frequency weight W_2 increases (W_1 = constant), $W_2\Delta f$ increases and is minimized by the MPC1 procedure. Therefore, the frequency deviation Δf reduced more than the indoor temperature deviation ΔT. The red dotted lines indicate that a large

frequency weight W_2 produces a small frequency deviation Δf, a large indoor temperature deviation ΔT. For simplicity, the signs (±) of the indoor temperature deviation ΔT and microgrid frequency deviation Δf are not considered. The signs of the indoor temperature and frequency deviations are shown in the subsection on tuning the temperature and frequency weights [48].

CHAPTER III

RESEARCH METHODOLOGY

This chapter introduces the research methodology. First, the problem formulation and modeling of the study system is explained. Next, the proposed improved resilient model predictive control (IR – MPC) for virtual inertia emulation by virtual energy storage system (VESS) under denial of service (DoS) attacks is introduced. Finally, the proposed enhanced resilient model predictive control (ER – MPC) based proton exchange membrane electrolyzers (PEMEL) control for frequency regulations under severe DoS attacks is explained.

Problem Formulation and Modeling of The Study Microgrid

In this section the problem formulation and modeling of the study microgrid is explained. First, microgrid control under DoS attacks is introduced. Next, the introduction to power system virtual inertia emulation is explained. Then, the microgrid model for virtual inertia control is described. Finally, the denial – of – service attacks modeling is described.

Microgrid Control Under DoS Attacks

In a microgrid, the controller is strategically positioned near distributed resources such as wind turbines, photovoltaic generators, inverter air conditioners, and virtual energy storage systems [49]. By receiving signals from the sensors and transmitting them to the distributed controller, the dynamic performance of the microgrid can be significantly improved. However, communication networks are prone to cyberattacks, which can negatively impact the stability, operation, and control of microgrids.

The main aim of this study is to improve the functionality of microgrid control systems in the face of distributed denial – of – service (DoS) attacks that target communication services in the transmission channel between the “Sensor” and “Controller” blocks, as shown in Figure 24. These attacks can disrupt communication

services [50], which can negatively impact the performance of controllers during the attacks. To address this issue, the proposed solution is an improved resilient model predictive control (IR – MPC) system that includes an "Attack detector" blocks to detect DoS attacks on the cyber – physical system and enhance the effectiveness of control actions.

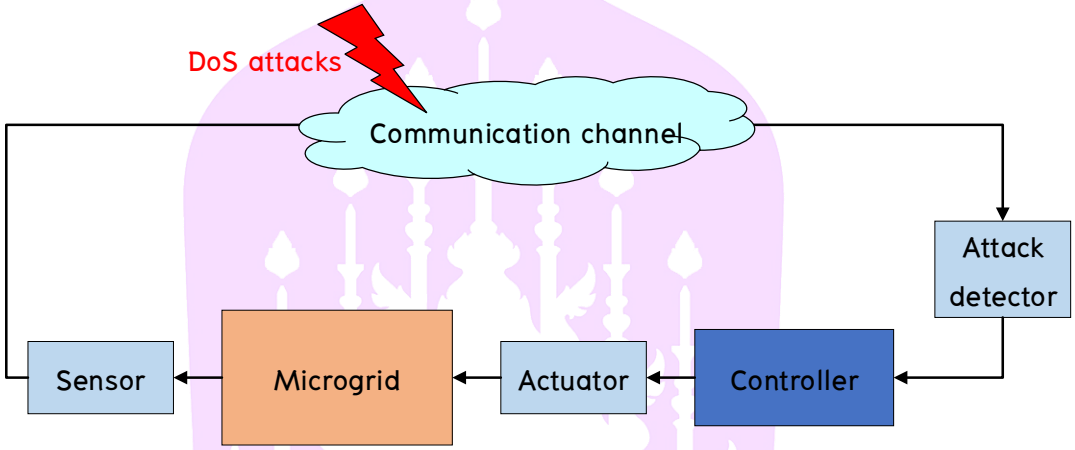


Figure 24 Microgrid control under DoS attacks.

Introduction to Power System Virtual Inertia Emulation

The inertia of a typical power system refers to the rotating mass of its synchronous generators, which are connected to the power system network. The speed of this mass changes in response to changes in demand and supply. However, the increasing number of renewable – based distributed generators connected to power systems via inertia – less power electronic inverters is leading to a reduction in power system inertia. To address this issue, the emulation of virtual inertia from an inverter is a promising solution. Additionally, smart loads, such as smart air conditioners connected to the grid via inverters, can be used for virtual inertia emulation [48].

As explained in [23], a power electronic inverter was used to emulate the swing equation of synchronous generator to implement a virtual inertia control. The following is an expression for the synchronous generator swing in Equation (59).

$$\overline{P}_m - \overline{P}_e = \frac{2H}{\omega_0}\frac{d^2\delta}{dt^2} = \frac{2H}{\omega_0}\frac{d\Delta\omega_r}{dt} \quad (59)$$

where

$\overline{P}_m$ and $\overline{P}_e$ are the mechanical and electrical powers of the synchronous generator,

H is the inertia constant,

ω_0 and ω_r are the rated angular and angular velocities of the rotor,

δ is the rotor angle,

t is the time.

When the damping component with the damping coefficient K_D is included, Equation (59) becomes.

$$\overline{P}_m - \overline{P}_e = \frac{2H}{\omega_0}\frac{d\Delta\omega_r}{dt} + K_D\frac{\Delta\omega_r}{\omega_0} \quad (60)$$

For load frequency control problems, the angular velocity deviation ($\Delta\omega_r$) was changed to the frequency deviation (Δf). Thus, Equation (60) can be represented as Equation (61).

$$\overline{P}_m - \overline{P}_e = \frac{2H}{f_0}\frac{d\Delta f}{dt} + K_D\frac{\Delta f}{f_0} \quad (61)$$

where

f_0 and f are the rated and instantaneous frequencies of the power system,

$d\Delta f / dt$ is the power system rate – of – change – of – frequency (RoCoF).

Microgrid Model for Virtual Inertia Control

Virtual inertia refers to the inertial support provided by distributed non – synchronous generation, energy storage devices, or smart loads that resemble the inertial response of a conventional power plant with the aid of appropriate control techniques and power electronic interfaces [51]. The microgrid in question comprises a diesel power plant (DS), wind turbine generators (WTG), photovoltaic generators (PV), inverter air conditioners (IACs), and conventional loads. The primary source of inertia for the microgrid is the synchronous machine representation, which includes the governor and rotor inertia of the diesel power plant. WTG, PV, and IACs are integrated into the microgrid through power electronic converters, which typically have low and zero inertia [52]. Notably, no inertia or damping controllers were installed in any of the power generators. Consequently, the operation of the microgrid is significantly affected by wind and PV power generation, which reduces the inertia and damping characteristics of the system. This, in turn, compromises the stability and performance of the microgrid. To address this issue, a virtual energy storage system (VESS) was employed to provide the microgrid with virtual inertia and frequency regulation services. A VESS is a combination of PV power generation and inverter air conditioners. If the generated power is less than the load, the speed and frequency of the generator unit will decrease. Conversely, if the generated power surpasses the load, the speed and frequency of the generator units increase. The microgrid frequency deviation (Δf) can be obtained using Equation (62).

$$\Delta f = \frac{1}{2Hs + D}\left(\underbrace{\Delta P_{DS} + \Delta P_{PV} + \Delta P_{WTG}}_{\text{generated power}} \underbrace{-\Delta P_{Load} - \Delta P_{IAC}}_{\text{demanded power}} \right) \tag{62}$$

where

H and D are the inertial and damping properties of the microgrid,

ΔP_{DS} is the power deviation of the diesel generator,

ΔP_{PV} is the power deviation of photovoltaic generators,

ΔP_{WTG} is the power deviation of the wind turbine generators,

ΔP_{Load} is the power deviation of the load demand,

ΔP_{IAC} is the power deviation of the inverter air conditioner.

The rate of change of the frequency or RoCoF of the microgrid can be defined using Equation (63).

$$R = \frac{d\Delta f}{dt} = \frac{\Delta f(t) - \Delta f(t_p)}{t - t_p}, \quad t > t_p \tag{63}$$

where

R is a short symbol of RoCoF,

t and t_p are represent the current and previous simulation times,

$\Delta f(t)$ and $\Delta f(t_p)$ are the frequency deviations at the current time t and the previous time t_p.

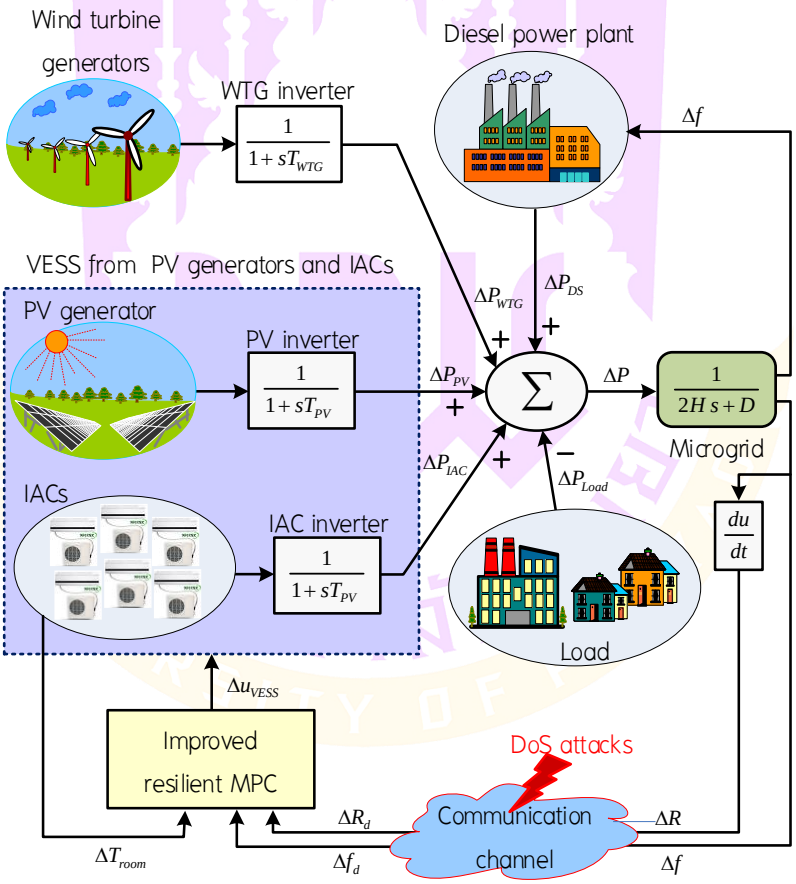


Figure 25 Microgrid with the proposed IR – MPC for virtual inertia control using VESS from PV generator and IACs under DoS attacks.

The study applied IR – MPC to control a virtual energy storage system (VESS) made up of inverter air conditioners and photovoltaic generators, simulating virtual inertia during DoS attacks.

1. Enhancing the virtual inertia emulator.

2. Managing frequency deviation.

3. The primary purpose of inverter air conditioners is to control indoor temperature.

4. Minimizing DoS attacks effects on virtual inertia and frequency regulation controllers.

The diesel power plant was located near the center of the control. The frequency deviation (Δf) is transmitted to a diesel power plant through a short transmission line. The effects of DoS attacks are not taken into account when it comes to the frequency control of diesel power plants, and thus, this study does not analyze the impact of such attacks on the control of diesel power plants.

Denial – of – Service Attacks Modeling

One of the most serious security concerns in cyber – physical systems is denial – of – service (DoS) attacks [53]. The use of deceptive and useless data by DoS attacks aims to deplete or utilize restricted resources in the power system components. The occurrence of a DoS attacks is signified by Equation (64).

$$\Im(0,\infty) \triangleq \bigcup_{l\in\mathbb{N}} [T_{on,l}, T_{off,l}] \tag{64}$$

where

T denotes the sampling period,

$T_{on,l} \in [T_{on}^{min}, T], l \in \mathbb{N}$ denotes the time at which a DoS attacks first occurs,

$T_{off,l} \in [T_{off}^{min}, T], l \in \mathbb{N}$ indicates the moment when the DoS attacks is over.

The trigger time for each DoS attacks was $T_{on} < T_{off} \leq T$, and the attacks duration was $T_{off} - T_{on}$. The equation for a nonperiodic random variable denial – of – service (DoS) attacks across all activation times is defined as Equation (65).

$$S_{DoS}(t) = \begin{cases} 0, & t \in \mathfrak{I}(0,\infty) \\ 1, & t \notin \mathfrak{I}(0,\infty) \end{cases} \tag{65}$$

where

$S = 0$ denotes the occurrence of DoS attacks,

$S = 1$ denotes normal transmission.

Detecting DoS attacks is a critical process in cyber – physical systems. These attacks can be prevented through local methods that protect potential victims or remote methods that detect spreading attacks [53].

Attack detection was executed close to the IR – MPC – based VESS controller. The method outlined in [53] was utilized to identify DoS attacks. Moreover, the RoCoF and frequency signals originating from the microgrid sensor were sent via the communication channel to the distributed IR – MPC – based VESS controller. These signals carry RoCoF and frequency deviations that manifest under DoS attacks. Therefore, accurate predictions of the RoCoF and frequency deviations are necessary to enhance the performance of the MPC. In the following subsection, the autoregressive (AR) models utilized to forecast RoCoF and frequency signals during DoS attacks are detailed.

IR – MPC for Virtual Inertia Emulation by VESS Under DoS Attacks

The proposed improved resilient model predictive control (IR – MPC) system for virtual inertia emulation in the presence of denial of service (DoS) attacks is explained in this section. It begins by outlining the virtual energy storage system (VESS) model. Then the autoregressive (AR) model – based prediction of two key metrics: the rate – of – change – of – frequency (RoCoF) and the frequency deviations during DoS incidents, is described.

The next step is to present the correlation coefficients for the time – series prediction data. Tuning of the autoregressive model weights is subsequently described in the text. Lastly, the IR – MPC system for virtual inertia emulation using a virtual energy storage system (VESS) is explained in detail.

Virtual Energy Storage System Model

The expense of conventional energy storage systems (ESS) can be quite high; therefore, a virtual energy storage system (VESS) is often used to enhance virtual inertia control in the face of DoS attacks. A VESS is composed of various electrical components that can be controlled, such as distributed generators, flexible loads, and energy storage devices. The VESS can absorb or release power to eliminate the fluctuations in power output that are typical of renewable energy sources [11], decrease frequency deviations, and provide virtual inertial control [48].

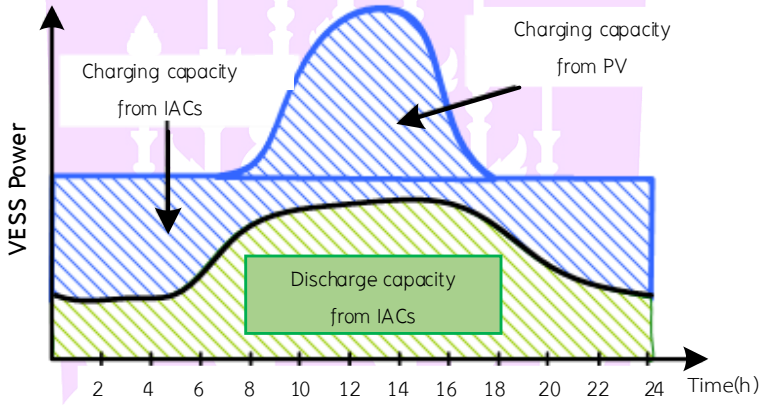


Figure 26 Capacity of virtual energy storage system from inverter air conditioner and photovoltaic generator.

The inverter – air conditioners and photovoltaic generators were combined and utilized as the VESS to provide virtual inertia control and frequency regulation using an IRMPC controller. The capacity of these devices was sufficient to support virtual inertia throughout the day, with inverter – air conditioners providing the necessary support during the night, and both inverter – air conditioners and photovoltaic generators providing support during the day.

The PV system generates power during the day, discharges power during the day, and cannot support a virtual inertial emulator at night. The IAC consumes low power during the night and high power during the day. The IAC has a very low

charging capacity during the day, which may not support a virtual – inertia emulator. Thus, the capacity of the VESS from the IACs and photovoltaic generator was adequate to sustain the virtual inertial emulator throughout the day.

The IR – MPC for Virtual Inertia Emulation by VESS

The MPC is an adaptive optimal control method that optimizes the control signal at each time instant. A resilient MPC (RMPC) was proposed in [54] to mitigate the MPC control effect during cyberattacks. The IR – MPC – based VESS controller comprises MPC1 and MPC2.

MPC1 was used to simultaneously control indoor temperature deviation (ΔT_{indoor}) and regulate microgrid frequency deviation ($\Delta\tilde{f}$). Consequently, the sum of the room temperature deviation and weighted frequency deviation served as MPC1's input, that is ($\Delta T_{indoor} + w_1\Delta\tilde{f}$). The selection of the frequency weight w_1 is important because the minimal and maximal temperature deviations, and the minimal and maximal frequency deviations are affected by the frequency weight w_1. The main idea is to increase the frequency deviation in the range of p.u.. This work uses $w_1 = 100$.

MPC2 is used to control the virtual inertia of the microgrid by controlling the initial gain of the VESS (K_{VI}). The RoCoF deviation ($\Delta\tilde{R}$) was used as the input, whereas K_{VI} was used as the output of MPC2.

When a DoS attacks occurs, the frequency and RoCoF deviations deteriorate, and the ability of the conventional MPC – based VESS to control the virtual inertia weakens. Consequently, an improved resilient MPC – based VESS was developed for the virtual inertia emulation. The block "Attack detector and signal estimator" is included in the preprocessing of the frequency deviation signal before sending it to the MPCs.

Additionally, the control signals of conventional resilient control methods are predicted or held during cyberattacks [50, 55 – 57]. However, owing to the multi – objective control of the MPC – based VESS, the predicted control signal (Δu_{VESS}) cannot be used during the DoS attacks. The VESS control signal was calculated using the indoor temperature, microgrid frequency deviation, and RoCoF deviation as inputs of the IR – MPC controller.

The indoor temperature is a local signal measured near the IRMCP controller and not sent through the communication link. DoS attacks do not deteriorate the indoor temperature signals. Thus, the original indoor temperature signal can be used as input to the IR – MPC during DoS attacks.

In contrast, the microgrid frequency deviation and RoCoF deviation are sent from the microgrid control center through the communication link. Therefore, a DoS attacks deteriorates the microgrid frequency deviation and the RoCoF deviation signals. Consequently, the attacks detector and signal estimator were applied to predict the microgrid frequency and RoCoF deviation signals during DoS attacks.

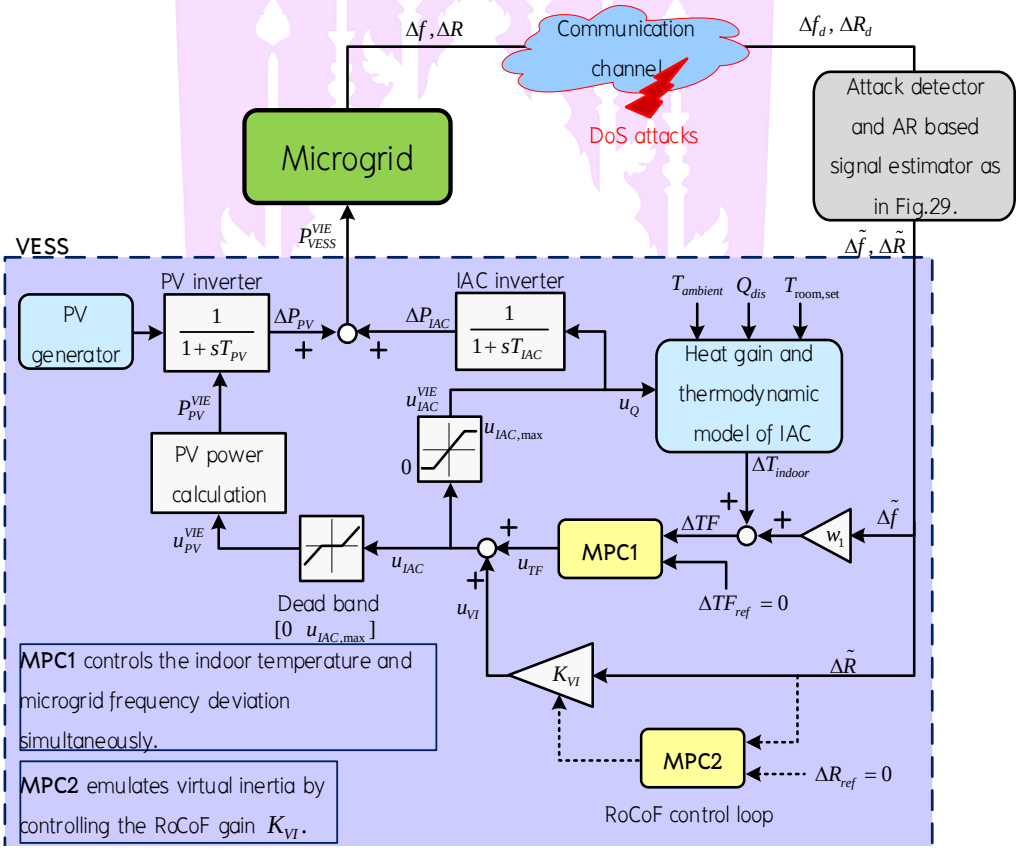


Figure 27 Proposed improved resilient model predictive control for virtual inertia emulation by virtual energy storage system under DoS attacks.

Autoregressive Model – based Prediction of RoCoF and Frequency Deviations

Autoregressive (AR) models are conventional statistical techniques that can be used to predict time – series data [23, 24]. The current output of an AR stochastic process is linearly dependent on past outputs. The definition of an AR model of order p is given by Equation (66).

$$x_t = \sum_{k=1}^{p} h_k x_{t-k} + \varepsilon_t \tag{66}$$

where

$x_t \in \mathbb{R}$ is the autoregressive model output,

h_k is the autoregressive coefficient for the k^{th} lag,

t is a time step,

$\varepsilon_t \in \mathbb{R}$ is the noise of the process, which is often assumed to be a zero – mean Gaussian variable with a finite variance σ^2.

The memory length of the autoregressive model p was captured by its order. The number of prior outputs on which the current output depends is measured by the memory length, p. The expected value of x_t can be defined using Equation (67).

$$\tilde{x}_t = \sum_{k=1}^{p} h_k x_{t-k} \tag{67}$$

Which along with σ^2 parameterizes the predictive distribution of $\{x_t\} \sim N(\tilde{x}_t, \sigma^2)$ conditional on the p previous measurement. The AR model was used to predict the RoCoF deviation (ΔR) and frequency deviation (Δf) feedback signals during a DoS attacks. The AR model for predicting RoCoF deviation can be expressed as Equation (68).

$$\Delta\tilde{R}(t) = \sum_{k=1}^{p_1} a_k \Delta R_d(t-k) \tag{68}$$

where

$\Delta\tilde{R}(t)$ is the predicted RoCoF deviation at time t,

p_1 is the order of the AR model for the prediction of RoCoF deviation,

a_k is the weight of the AR models for predicting the RoCoF deviation,

ΔR_d is the RoCoF deviation that is transmitted through the communication link and damaged by DoS attacks.

The AR model for the prediction of the frequency deviation can be defined by Equation (69).

$$\Delta\tilde{f}(t) = \sum_{k=1}^{p_2} b_k \Delta f_d(t-k) \tag{69}$$

where

$\Delta\tilde{f}(t)$ is the predicted frequency deviation at time t,

p_2 is the order of the AR model for predicting frequency deviation,

b_k is the weight of the AR model for predicting frequency deviation,

Δf_d is the frequency deviation transmitted through the communication link that is damaged by the DoS attacks.

Correlation Coefficient of the Time Series Prediction Data

The correlation coefficient is a statistical concept that helps establish the relationship between the predicted and actual values obtained in a statistical experiment [58]. The calculated value of the correlation coefficient explained the difference between the predicted and actual values. The correlation coefficient always lies between −1 and +1. If the correlation coefficient is positive, there is a similar and identical relationship between the two variables.

The correlation coefficient of two random variables is a measure of their linear dependence. If each variable has scalar observations, the Pearson correlation coefficient is defined as Equation (70).

$$\rho(A,B) = \frac{1}{N-1}\sum_{i=1}^{N}\left(\frac{A_i - \mu_A}{\sigma_A}\right)\left(\frac{B_i - \mu_B}{\sigma_B}\right) \tag{70}$$

where

μ_A and σ_A are the mean and standard deviation of variable A, respectively,

μ_B and σ_B are the mean and standard deviation of variable B, respectively.

Alternatively, the correlation coefficient in terms of the covariance of A and B can be defined using Equation (71).

$$\rho(A,B) = \frac{\mathrm{cov}(A,B)}{\sigma_A \sigma_B} \tag{71}$$

In this research, the correlation coefficient was employed to determine the relationship between the current signal and the delay signal, which can be utilized to select the order of the AR models.

Autoregressive Model Weight Tuning

The AR models weights (a_k and b_k) for the prediction of the RoCoF and frequency deviations were tuned simultaneously using a firefly algorithm (FLA) [26]. The objective function is the summation of the integral absolute error (IAE) of the frequency deviation [59] and RoCoF deviation. Thus, the objective function can be expressed by Equation (72).

$$\begin{aligned} &\text{Minimize IAE} = \int_{t_s}^{t_e} |\Delta f| dt + \int_{t_s}^{t_e} |\Delta R| dt \\ &\text{Subject to} \quad a_{k,min} \le a_k \le a_{k,max}, \\ &\qquad\qquad b_{k,min} \le b_k \le b_{k,max}, \quad k = 1,2,\ldots,p. \end{aligned} \tag{72}$$

where

t_s and t_e are the start and end times of the simulations respectively,

$a_{k,min}$ and $a_{k,max}$ are the minimum and maximum weights of the AR models, respectively, for predicting the RoCoF deviation,

$b_{k,min}$ and $b_{k,max}$ are the minimum and maximum weights of the AR models for predicting the frequency deviation respectively,

k is the number of AR models used.

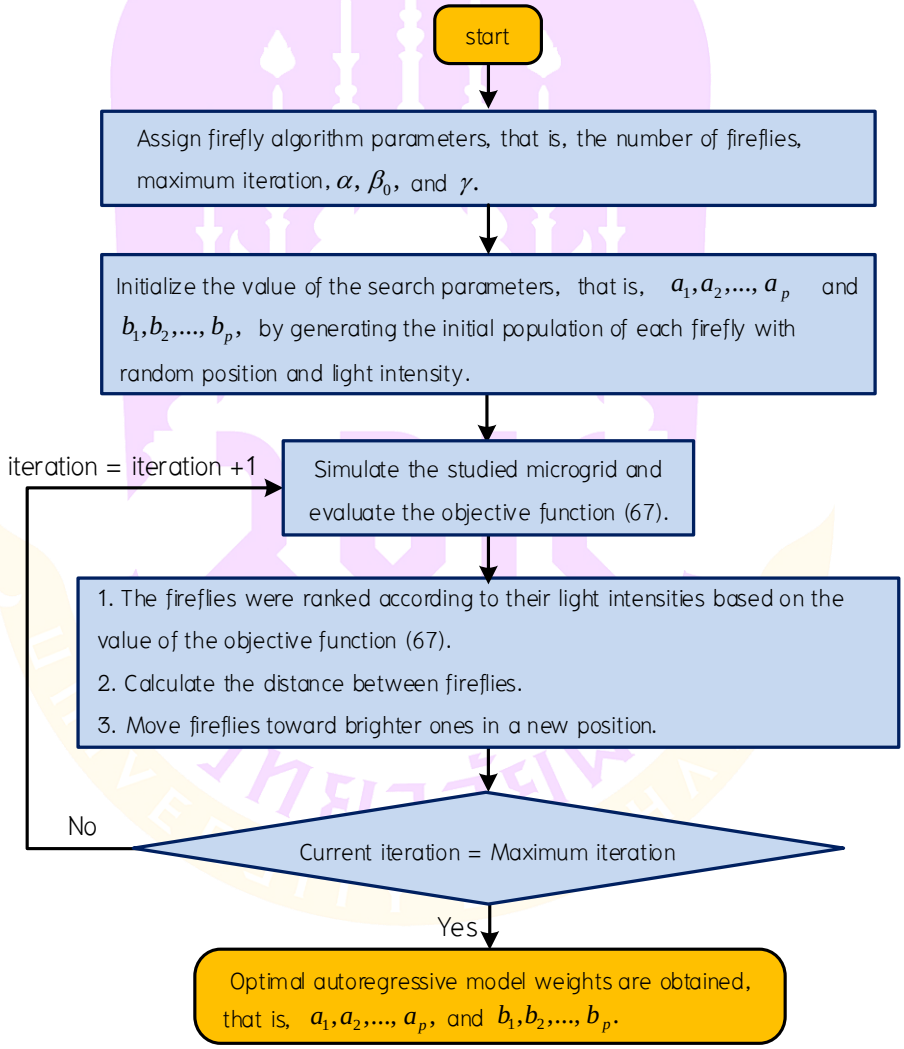


Figure 28 The autoregressive model weight tuning using firefly algorithm.

The procedure for the autoregressive model weight tuning using the firefly algorithm is shown in Figure 27. Where γ is the light absorption coefficient of the firefly, α is the randomization parameter, β_0 is the attractiveness of the firefly algorithm at iteration 0 [26].

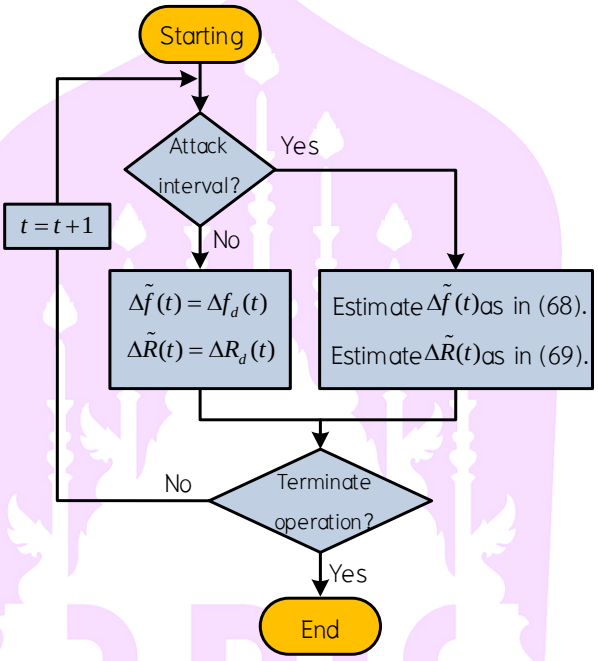


Figure 29 Attacks detector and autoregressive model – based signal estimator.

Figure 29 shows the attacks detector and autoregressive model – based signal estimator, which are used to predict the microgrid frequency deviation and RoCoF deviation signals during the DoS attacks.

Proposed ER – MPC for PEMEL Control under Severe DoS Attacks

This section describes the enhanced robust model predictive control – based PEMEL controller that is suggested for use in the event of major DoS attacks on microgrid frequency auxiliary services. Firstly, we describe how to estimate the frequency deviation, or feedback signal, in the event of a DoS attacks. Subsequently, a description of the enhanced resilient model predictive control for PEMEL frequency regulation control is provided.

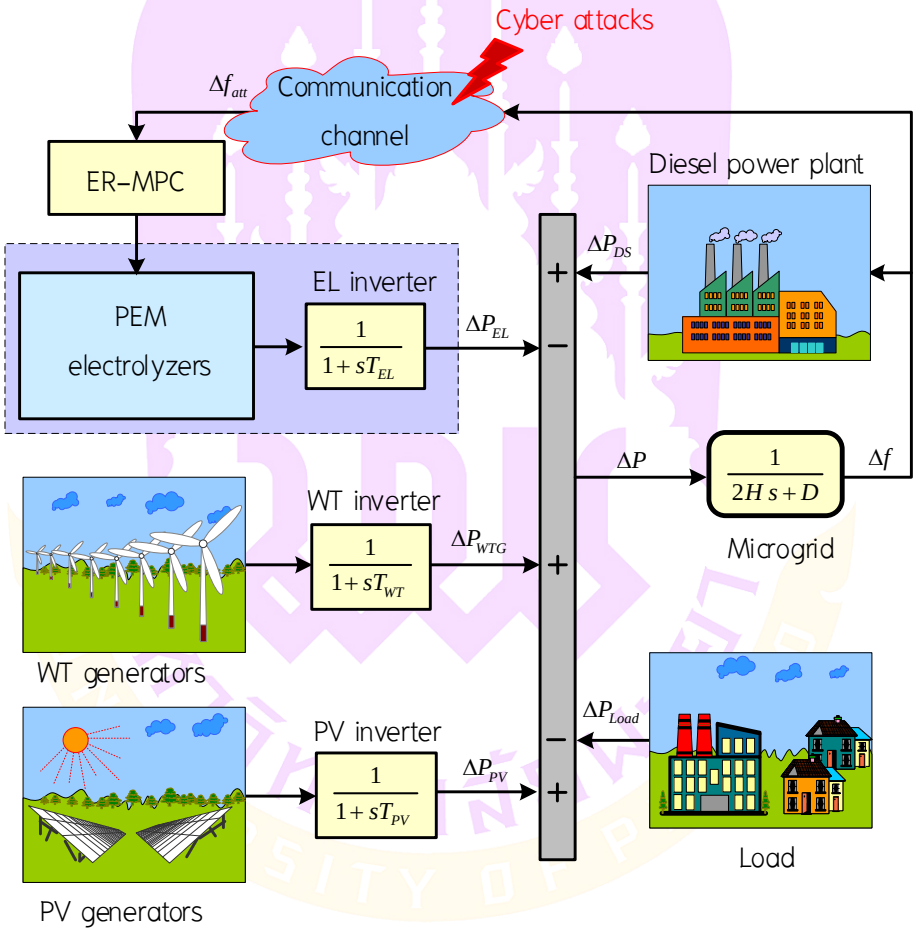


Figure 30 Microgrid with the proposed ER – MPC – based PEMEL for virtual inertia and frequency regulations under DoS attacks.

Microgrid Model for Frequency Control Under DoS Attacks

First, a microgrid frequency regulation model under cyberattacks is introduced. Next, we explain the PEMEL model for frequency regulation. Subsequently, the control of a large – scale PEMEL stack was proposed. Finally, the DoS attacks model is explained.

Figure 30 depicts the microgrid with the proposed enhanced resilient MPC – based PEMEL for frequency regulation during DoS attacks. In the transmission channel between the "Microgrid" and "PEMEL controller" blocks, DoS attacks were employed to disrupt communication services, which harms system functionality [60]. Controller performance may suffer during a DoS attacks. As a result, the ER – MPC and the PEMEL controller ought to be built to reduce the impact of a DoS attacks on control actions. To improve microgrid frequency regulation during DoS attacks, this study suggests an improved resilient model predictive control for proton exchange membrane electrolyzers. As shown in Figure 30, the microgrid frequency deviation can be expressed as Equations (73) – (74).

$$\Delta f = \frac{1}{2Hs + D}\Delta P \tag{73}$$

$$\Delta P = \Delta P_{DS} + \Delta P_{PV} + \Delta P_{WTG} - \Delta P_{Load} - \Delta P_{EL} \tag{74}$$

where

H stands for the microgrid's inertia,

D for its damping qualities,

P_{DS} for the diesel generators power,

P_{PV} for the photovoltaic generators power,

P_{WTG} for the wind turbine generators power,

P_{Load} for the load demand's power,

P_{EL} for the PEMEL's power,

Δ is the deviation of the signal.

The nominal system frequency varies because of the discrepancy between the generated power and load demand. If the generated power is less than the load, the generator units' speed and frequency begin to decrease $(-\Delta P)$. The generators frequency and speed started to increase when the generated power surpassed the load $(+\Delta P)$.

The frequency deviation caused by the intermittent nature of renewable energies, such as photovoltaic generators and wind power generation, as shown in Figure 30, can be reduced by controlling the PEMEL. However, owing to the distribution control of microgrids through communication channels, cyberattacks may deteriorate the control performance of the PEMEL to suppress frequency fluctuations. Thus, an enhanced resilient model predictive control has been used to control PEMEL.

In addition, the diesel power plant is thought to be situated near the control center. Consequently, the effect of DoS attacks on the diesel power plant control was not considered in this study.

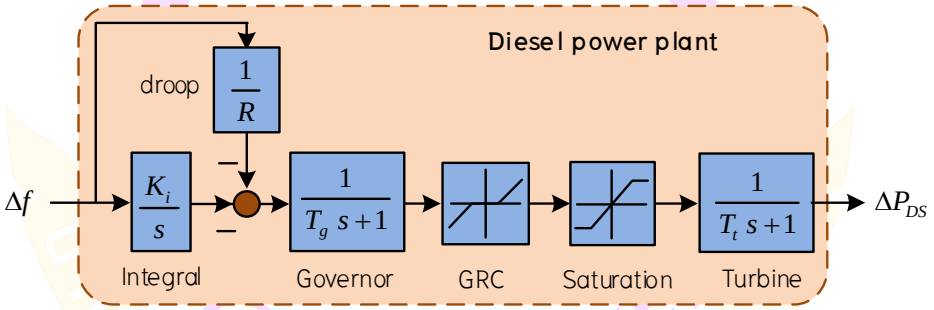


Figure 31 Diesel power plant model used in the study.

PEMEL Model for Frequency Regulations

Hydrogen electrolysis is a power – to – gas storage technology that facilitates the integration of intermittent renewable energy sources into future energy systems on a wide scale. Figure 32 shows the dynamic properties of a PEMEL stack, which is based on the dynamic electrical equivalent model for frequency regulation.

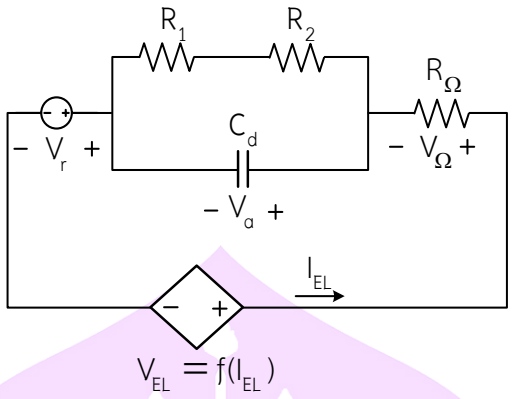


Figure 32 PEMEL dynamical electrical equivalent circuit.

The following first – order differential equation can be used to express the dynamic properties of the circuit shown in Figure 32.

$$\frac{dV_a}{dt} = \frac{I_{EL}}{C_d} - \frac{V_a}{T_{EL}} \tag{75}$$

where

V_a is the activation voltage drop,

I_{EL} is the PEMEL current,

C_d is the capacitor,

T_{EL} is the first – order time constant of the PEMEL.

The cathodic/anodic electrode separating two different types of materials causes T_{EL} due to charge accumulation/decumulation brought on by electrons moving from one electrode to another. T_{EL} also known as the charge double – layer effect and can be expresses as follows [61, 62].

$$T_{EL} = (R_1 + R_2)C_d = R_d C_d \tag{76}$$

where

R_1 and R_2 are the PEMEL resistances showing the activation losses,

R_d is the equivalent resistance,

C_d is a change in the electrolyzer current that can dynamically affect the PEMEL or charge layer at the electrode – electrolyte interface.

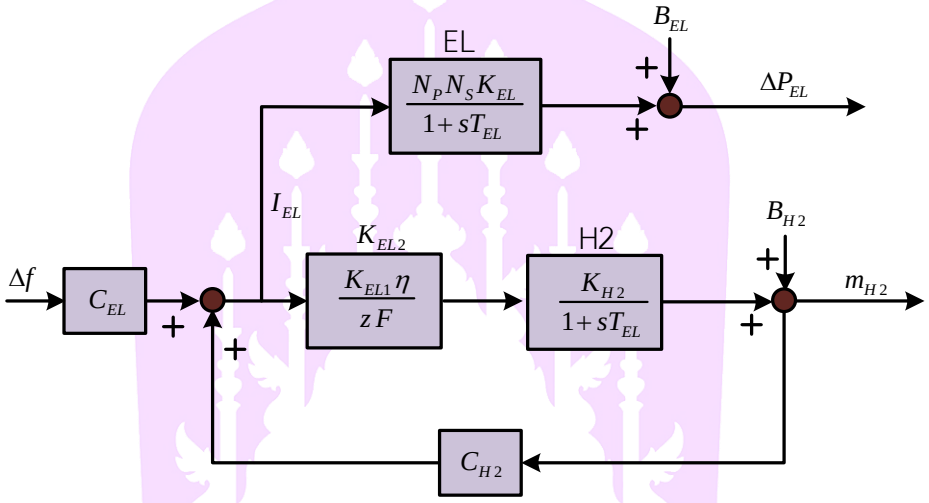


Figure 33 PEMEL model for frequency regulations used in this study.

The linearized model of the PEMEL for power system frequency regulation modified from [61] and [62] is shown in Figure 33. T_{EL} needs to be taken into account when using PEMEL to regulate power system frequency. The regulation and adjustment of the PEMEL power consumption are delayed by T_{EL} in event of rapid changes in the system frequency. Therefore, the power consumption of the PEMEL can be described by the Laplace transform as Equation (77).

$$P_{EL}(s) = \frac{K_{EL}}{1+sT_{EL}} I_{EL}(s) + B_{EL} \quad (77)$$

where

K_{EL} and B_{EL} are the coefficients and initial PEMEL power consumption, respectively.

The downstream hydrogen production rate m_{H2} [Nm^3 / s], can be expressed by Equation (78).

$$m_{H2}(s) = K_{EL1} \frac{\eta_F I_{EL}(s)}{zF} \tag{78}$$

where

K_{EL1} is the coefficient converts mole/s to Nm^3 / s,

z is the electron density, F is Faraday's constant,

η_F is stands for Faraday efficiency.

The time delay T_{EL} may change the hydrogen production sub – model since the rate of hydrogen synthesis is a linear function of current. Thus, the hydrogen production sub – model can be expressed as Equations (79) – (80).

$$m_{H2}(s) = \frac{K_{EL2} K_{H2}}{1 + sT_{EL}} I_{EL}(s) + B_{H2} \tag{79}$$

$$K_{EL2} = K_{EL1} (\frac{\eta_F}{zF}) \tag{80}$$

where

K_{H2} is the hydrogen coefficients,

B_{H2} is the initial hydrogen production rate.

Control of a PEMEL Stack

To produce the necessary output voltages, currents, and power for grid applications, a PEMEL stack was built using series – parallel connections. This can be represented by Equations (81) – (83).

$$V_{EL,stack} = N_S V_{EL} \tag{81}$$

$$I_{EL,stack} = N_P I_{cell} \tag{82}$$

$$P_{EL,stack} = V_{EL,stack} I_{EL,stack} \tag{83}$$

where

N_S and N_P are the numbers of series and parallel connected cells per stack, respectively.

The PEMEL stack current ($I_{EL,stack}$) can be adjusted to control the downstream hydrogen generation rate and power consumption. The aim of hydrogen production control is to maintain the regulated downstream rate of hydrogen generation. The difference between the current rate of hydrogen production, indicated by m_{pre}, and the previous value, indicated by m_{past}, is therefore used to change the downstream hydrogen generation rate of the PEMEL stack. This difference can be expressed by Equation (84).

$$\Delta m_{H2}(s) = m_{pre}(s) - m_{past}(s) \tag{84}$$

Thus, the PEMEL current deviation can be expressed by Equation (85).

$$\Delta I_{EL}(s) = C_{H2}(s) \cdot \Delta m_{H2}(s) \tag{85}$$

where

C_{H2} is a built – in controller that controls hydrogen production rate.

To provide the frequency regulation capacity, an additional controller, C_{EL}, is included to regulate the hydrogen generation rate for frequency regulation. Thus, can be revised as follows equation (86).

$$\Delta I_{EL}(s) = C_{H2}(s) \cdot \Delta m_{H2}(s) + C_{EL}(s) \cdot \Delta f(s) \tag{86}$$

where

Δf is stands for the power systems frequency deviations.

The PEMEL power adjustment was calculated by replacing Equation (86) in Equation (83) as follows Equation (87).

$$\left.\begin{aligned}\Delta P_{EL}(s) = \frac{K_{EL}}{1+sT_{EL}} C_{H2}(s)\cdot\Delta m_{H2}(s) \\ + \frac{K_{EL}}{1+sT_{EL}} C_{EL}(s)\cdot\Delta f(s)\end{aligned}\right\} \quad (87)$$

According to Equation (87), there are two parameters that are related to the PEMEL operational power adjustment Equation (72) the fluctuation in the rate of hydrogen generation (Δm_{H2}), and Equation (73) the variation in frequency (Δf). The rate of hydrogen production variation can be ignored because of the short duration of the frequency adjustment method (maximum of 30 s). Consequently, it is possible to regard the rate of hydrogen creation as constant during this time. Consequently, can be expressed simply as shown in Equation (88).

$$\Delta P_{EL}(s) = C_{EL}(s)\cdot\frac{K_{EL}}{1+sT_{EL}}\cdot\Delta f(s) \quad (88)$$

In this study, the ER – MPC is used to control the PEMEL for frequency regulation. Δf is the ER – MPC input which is used to compute control signal for PEMEL controller. Thus, when using ER – MPC to control PEMEL for frequency regulation, Equation (88) can be expressed as Equation (89).

$$\Delta P_{EL}(s) = u_{ER-MPC}(s)\cdot\frac{K_{EL}}{1+sT_{EL}} \quad (89)$$

In this study, we assumed that the ER – MPC controller was located close to the PEMEL stack. Thus, the DoS attacks caused Δf deteriorates and must be improved by the proposed ER – MPC.

Our research approach assumes that the ER – MPC controller is situated near the PEMEL stack, and we aim to address the performance degradation resulting from a Denial of Service (DoS) attacks by implementing the proposed ER – MPC.

Methods for Estimating Feedback Signal During DoS Attacks

Methods used in this study to estimate signals during DoS attacks. More details are provided below.

First: Hold Signal Technique. Figure 34 (a) shows the hold signal method [57] when the system encounters cyberattack. The holding signal method is defined by Equation (90).

$$\Delta\tilde{f}(t) = \Delta f(t-1) \tag{90}$$

where

$\Delta\tilde{f}(t)$ is the frequency deviation reconstructed by the holding method,

$\Delta f(t-1)$ is the actual frequency deviation at time $t-1$ which is transmitted through the communication link before the DoS attacks occurs.

The holding signal may deteriorate when the attacked signals are significantly different from the last known signal (i.e., when the hold signal is the same as the last known signal).

Second: Prediction Technique. In this study, an autoregressive (AR) model was used to predict frequency deviations (Δf) during a DoS attacks.

Conventional statistical methods, such as AR models, can be applied to time – series data prediction. The current output of an AR stochastic process depends linearly on the previous output. The AR model for the prediction of frequency deviation is defined by Equation (91) [60].

$$\Delta\tilde{f}(t) = \sum_{k=1}^{p} b_k \Delta f_{com}(t-k) \quad (91)$$

where

$\Delta\tilde{f}$ is the predicted frequency deviation,

t indicates the current time instant,

p is the order of the AR model,

b_k is the weight of the AR model,

Δf_{com} is the frequency deviation sent via a communication link that is harmed by DoS attacks.

Figure 34 (b) shows the prediction method using autoregressive model – based prediction [60]. Error in the prediction method may increase when the prediction samples are far from the last known signal. Therefore, the prediction method may deteriorate when it is used to predict an attack signal during a severe DoS attack.

Third: Predict and Hold Technique. To improve the performance of the reconstruction signal for a resilient MPC, the prediction and hold technique, as shown in Figure 34 (c), is proposed. The combination of the prediction method and hold signal method improves the performance of the control techniques owing to the long – time of unknown data during the DoS attack.

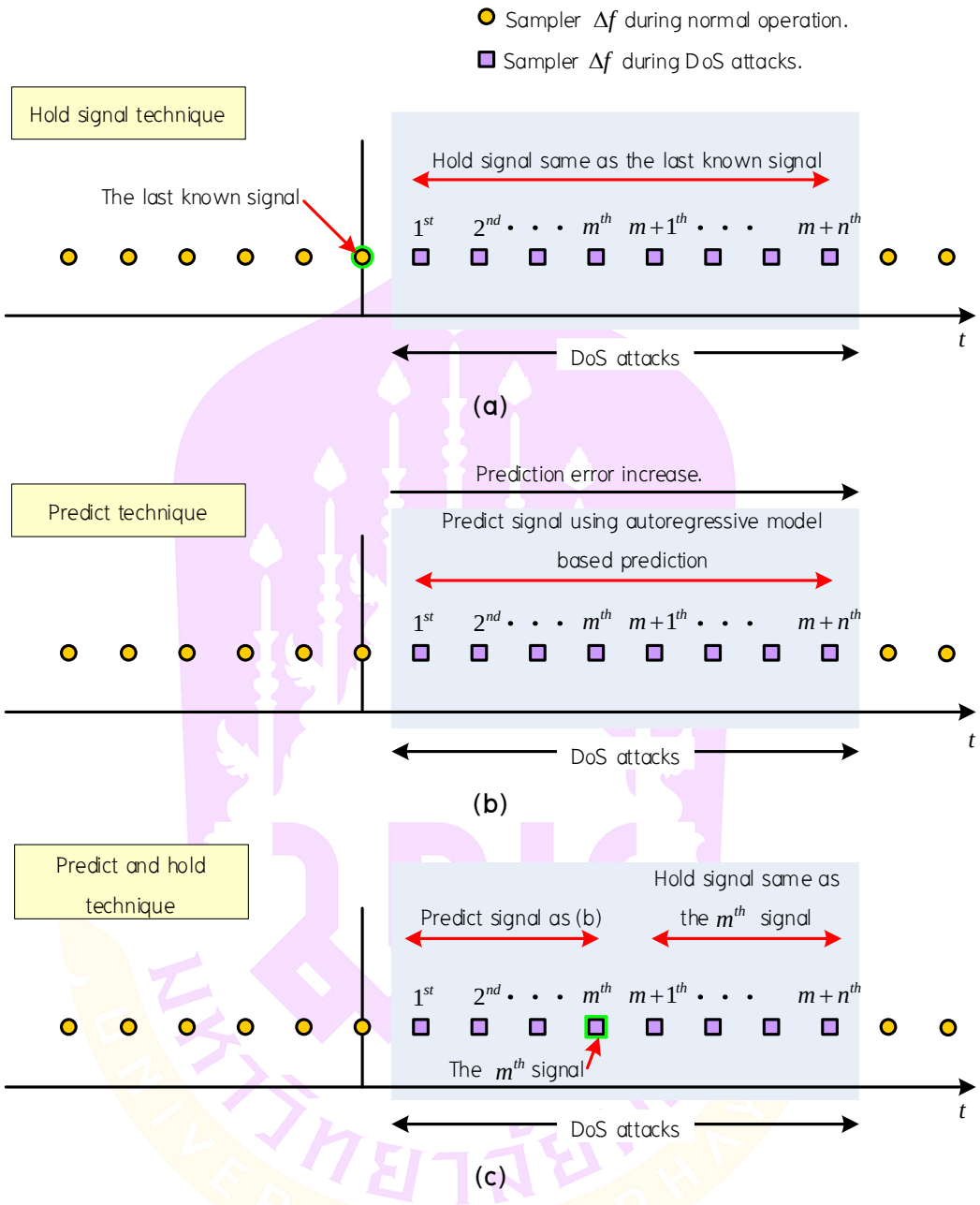


Figure 34 Methods for estimating signal during DoS attacks (a) hold signal technique (b) prediction technique (c) predict and hold technique.

Proposed ER – MPC – Based PEMEL Control for Frequency Regulations

The PEMEL controller receives frequency variation through a communication link that is vulnerable to DoS attacks. The frequency deviations worsen during a DoS attacks, and the traditional MPC – based PEMEL's capacity to control the frequency decreases. Therefore, as shown in Figure 35.

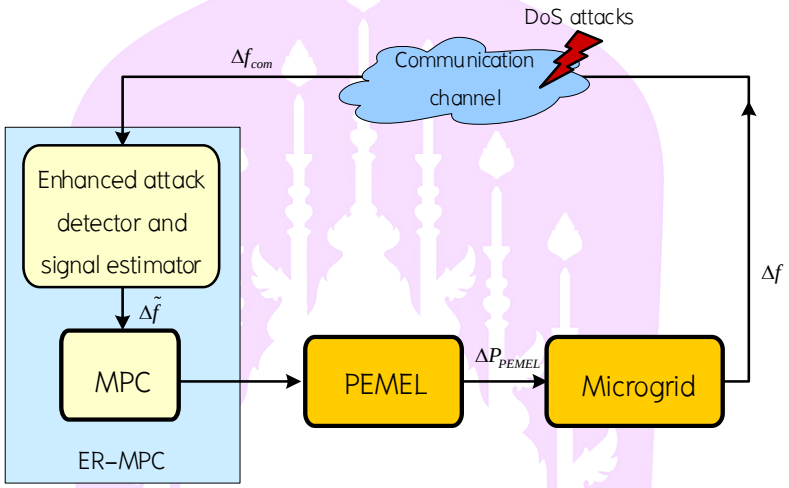


Figure 35 The proposed ER – MPC – based PEMEL control under DoS attacks.

Our study suggests an enhanced resilient MPC – based PEMEL for frequency regulation. Additionally, before the frequency deviation signal is sent to the MPCs, it is preprocessed with the block “Enhanced attack detector and signal estimator” as shown in Figure 36, added.

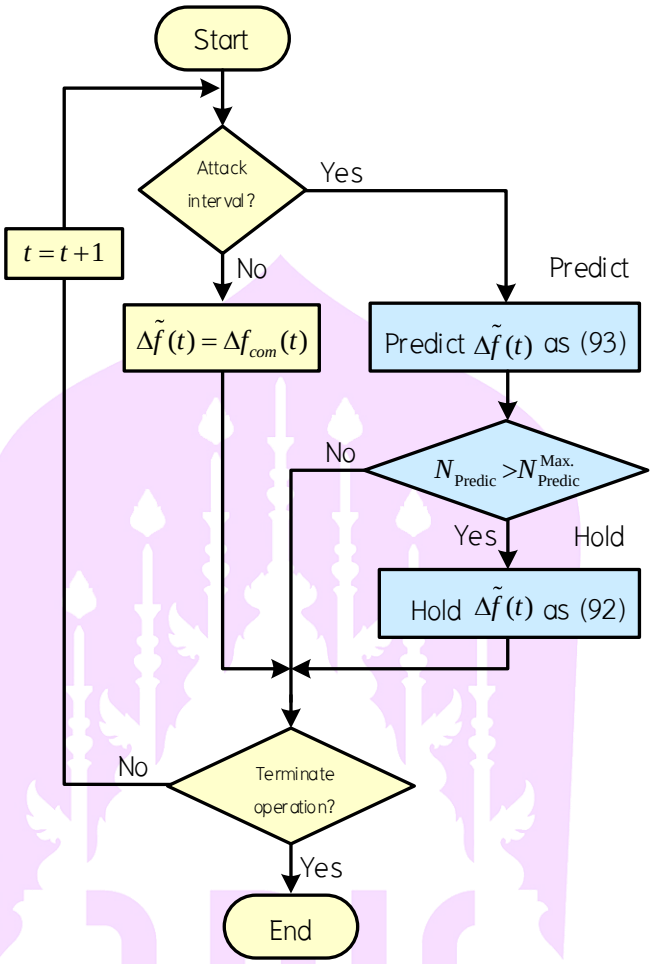


Figure 36 An enhanced attacks detector and signal estimator.

CHAPTER IV

RESULTS

This chapter explains the results of the study. First, the improved resilient model predictive control (IR – MPC) for enhanced microgrid virtual inertia emulation by virtual energy storage system (VESS) under denial of service (DoS) attacks is introduced. Next, Proton Exchange Membrane Electrolyzers (PEMEL) control for microgrid frequency regulations under severe DoS attacks using enhanced resilient MPC (ER – MPC) is explained.

IR – MPC for Enhanced Microgrid Virtual Inertia Emulation by Virtual Energy Storage System Under DoS Attacks

Simulation results and discussion are presented in this section. First, the study of the rate – of – change – of – frequency (RoCoF) and frequency deviation signals versus time delays is described, and then the simulation settings are explained. Subsequently, the simulation results and a discussion are presented.

Study RoCoF and Frequency Deviation Signals Versus Time Delays

The autoregressive (AR) model uses historical data to predict future events. By examining the connections between RoCoF and frequency deviation signals in relation to time delays, the model's ability to accurately forecast RoCoF and frequency deviation in the context of denial of service (DoS) attacks can be improved.

The relationship between the current RoCoF and delay RoCoF in subfigures A, B, and C is illustrated in the upper subfigure of figure 37. The positions of subfigures A, B, and C are shown in the time – domain simulation of the RoCoF. Sub – figure A displays a scatter plot of the current RoCoF and the delay RoCoF for approximately 150 seconds, covering the range of frequencies between –7.5 and –6.0 Hz/s. The different delays considered were 0, 1, 2, 3, and 4. A delay of 0 indicates that the current signal is plotted

against the same current signal, which makes it an ideal case for a regression problem, as shown by the black lines representing the data.

However, in the prediction signal during a DoS attack, the signal with a delay of 0 is unknown. The relationship between these delay signals and the current signal is studied. The signal with a delay of 1 is found to be closer to the black line than the signals with delays of 2, 3, etc. (as shown by the green dotted line). This suggests that a signal with delay of 1 can better predict a signal with delay of 0 compared to other signals. Additionally, when the delay time increased, the scatter plot spread out of the black line. Sub – figures A, B, and C show that the signals with time delays of 1 and 2 are suitable for use in the linear regression of the AR model of RoCoF prediction.

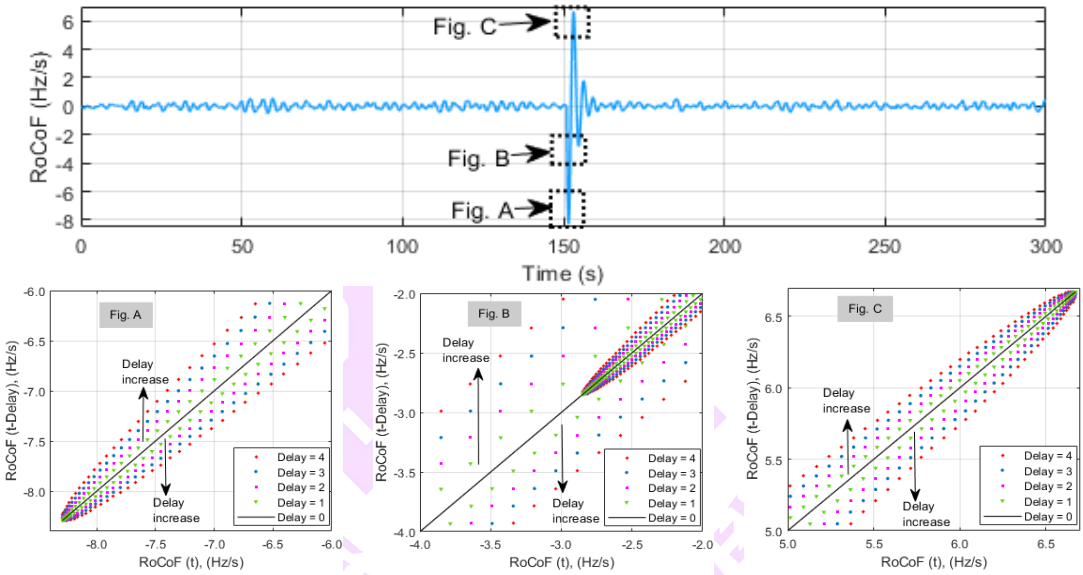


Figure 37 The relationship between current RoCoF (RoCoF(t)) and time delay RoCoF (RoCoF(t – Delay)).

Figure 38 shows the relationship between the frequency deviation and delay frequency deviation in subfigures A, B, and C. The upper figure shows the time – domain simulation of the frequency deviation, in which the positions of subfigures A, B, and C are located. The scatter plots in subfigures A, B, and C demonstrate that a signal with time delays = 1 and 2 is appropriate for use in the linear regression of the AR model for frequency deviation prediction.

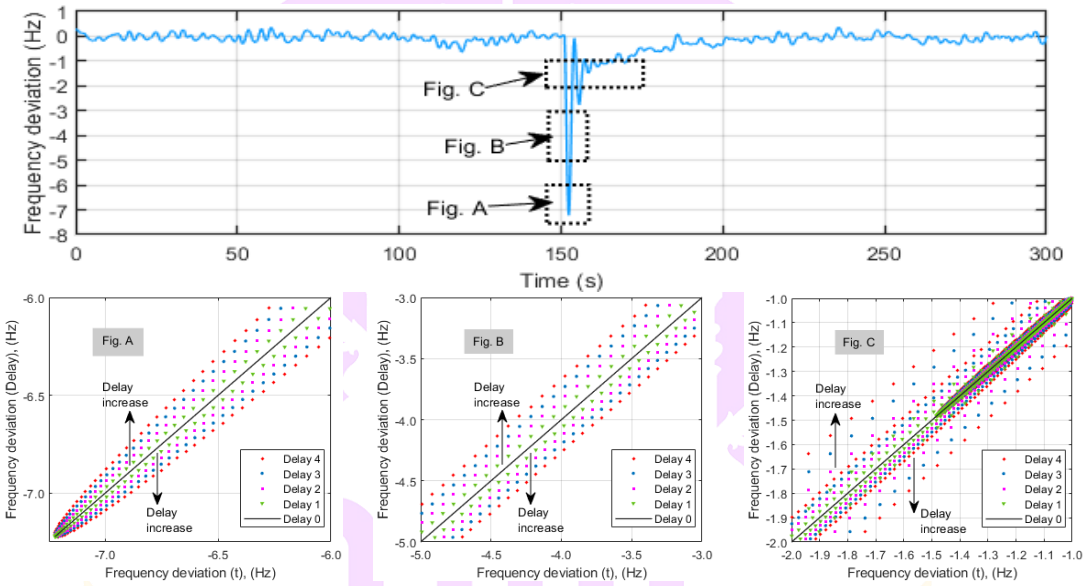


Figure 38 The relationship between current frequency deviation $(\Delta f(t))$ and time delay frequency deviation $(\Delta f(t-\text{Delay}))$.

Table 6 Correlation coefficient of delay RoCoF versus RoCoF with delay 0.

	Time of measured (s)						
Delay	0 – 150	150 – 160	160 – 170	170 – 180	180 – 190	190 – 200	200 – 300
0	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1	0.9997	0.9998	0.9997	0.9997	0.9998	0.9996	0.9997
2	0.9989	0.9991	0.9989	0.9989	0.9992	0.9986	0.9990
3	0.9976	0.9979	0.9976	0.9976	0.9981	0.9968	0.9977
4	0.9958	0.9964	0.9957	0.9958	0.9967	0.9944	0.9959

Table 6 shows the correlation coefficients of the RoCoF signal with time delays = 0, 1, 2, 3, and 4 against that of the time delay = 0. The RoCoF signal with delay = 0 compared to the RoCoF signal with delay = 0 (the same signal) has a correlation coefficient of 1. A correlation coefficient of 1 indicates perfect regression. When the RoCoF signal has delay = 1, the correlation coefficient near 1 appears to be a near – perfect regression. However, during the disconnection of the WTG at 150 – 200 s, the correlation coefficient was lower than that under normal operation at 0 – 150 s and 200 – 300 s. The correlation coefficients clearly decreased when the delay was greater than 3. Thus, signals with delays = 1 and 2 had a correlation coefficient close to that of delay = 0. Therefore, the AR model p=2 is appropriate for RoCoF prediction.

Table 7 Correlation coefficient of delay Δf versus Δf with delay 0.

	Time of measured (s)						
Delay	**0 – 150**	**150 – 160**	**160 – 170**	**170 – 180**	**180 – 190**	**190 – 200**	**200 – 300**
0	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1	0.9999	0.9999	0.9999	1.0000	0.9999	0.9999	0.9999
2	0.9997	0.9995	0.9996	0.9999	0.9998	0.9996	0.9996
3	0.9993	0.9988	0.9991	0.9997	0.9995	0.9991	0.9992
4	0.9988	0.9979	0.9984	0.9995	0.9991	0.9984	0.9986

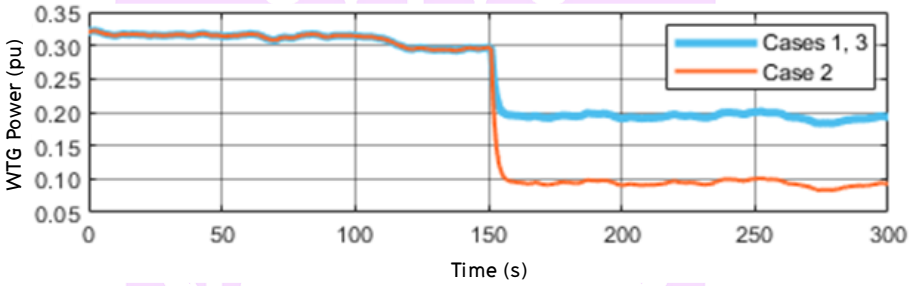
Table 7 shows the correlation coefficients of the frequency deviation signal with time delays = 0, 1, 2, 3, and 4 against that of time delay = 0. The frequency deviation signal with delay = 0 compared to the frequency deviation signal with delay = 0 (the same signal) has a correlation coefficient of 1. A correlation coefficient of 1 indicates perfect regression. When the frequency deviation signal with delay = 1, the correlation coefficient near 1 appears to be a near perfect regression.

However, during the disconnection of the WTG at 150 – 200 s, the correlation coefficient was lower than that under normal operation at 0 – 150 s and 200 – 300 s. The correlation coefficients clearly decreased when the delay was greater than 3.

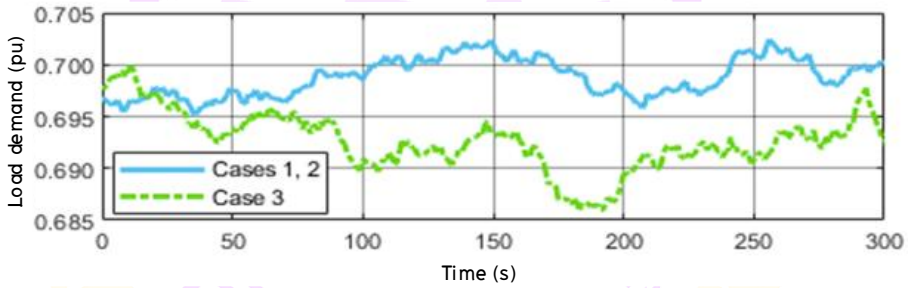
Thus, signals with delays = 1 and 2 had a correlation coefficient close to that of delay = 0. Therefore, the AR model p=2 is appropriate for frequency deviation prediction.

IR – MPC – based VESS Simulation Setting

The efficiency of the proposed IR – MPC for improving the microgrid virtual inertia when subjected to DoS attacks was assessed using MATLAB/Simulink. The MATLAB/Simulink MPC toolbox was used to perform MPC [63]. The microgrid, shown in Figure 25, was used as the study system. The microgrid data were obtained from [48].



(a)



(b)

Figure 39 WTG power and load demand of the case studies (a) WTG power (b) load demand.

Figure 39 (a) shows the wind turbine generation (WTG) for case studies. It is assumed that at 150 s, WTG disconnects 0.1 p.u., 0.2 p.u., and 0.1 p.u. for Cases 1, 2, and 3, respectively. The disconnection of the WTG causes a reduction in the inertia of the microgrid. Thus, RoCoF is higher than the nominal value and may reach the RoCoF maximum allowance limit. The load demands of the case studies are shown in

Figure 39 (b). The load demands of Cases 1 and 2 were higher than that of Case 3. However, the oscillation of the load demand in Case 3 was higher than those in Cases 1 and 2. The higher oscillation of the load demand in Case 3 can cause the frequency and RoCoF deviations to be higher than in Cases 1 and 2.

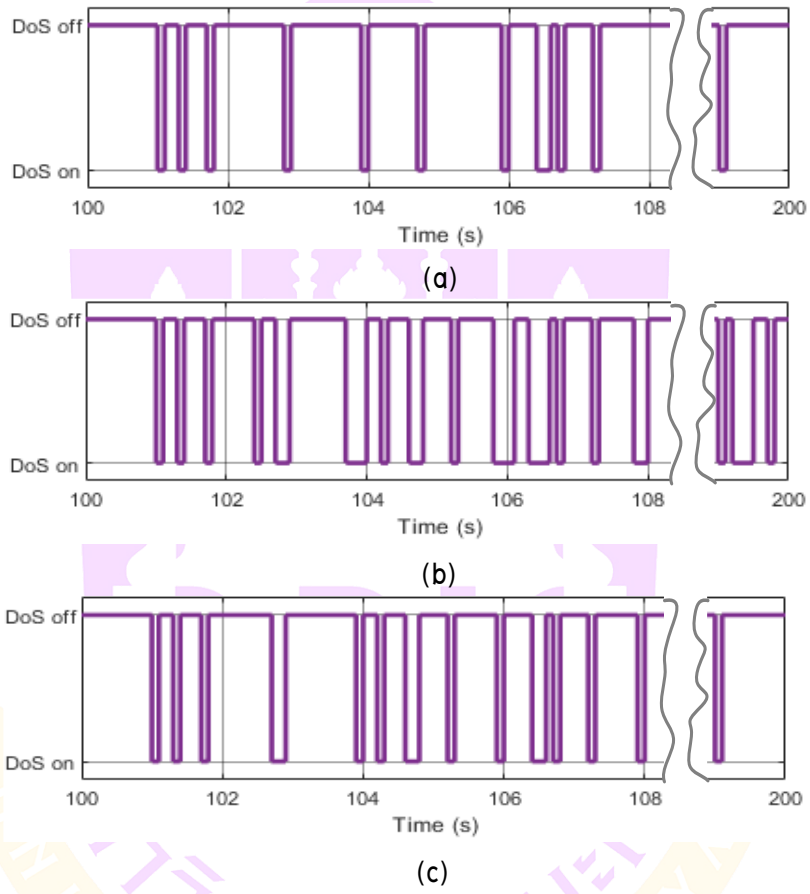


Figure 40 DoS attacks signal of the case study (a) Case 1 (b) Case 2 (c) Case 3.

Figure 40 shows the DoS attack signals used in the case study. The Bernoulli random variable was used to generate the DoS signals [64]. When using the MATLAB/Simulink toolbox, the DoS attack level can be changed by varying the probability of zero for a Bernoulli random variable. A probability of zero implies a probability of DoS attacks in the transmission system. If the probability of zero is zero,

it implies that there are no DoS attacks on the transmission system. If the probability of zero is one, this implies that many DoS attacks occur in the transmission system and none of the signals can be transmitted through the transmission link. In this study, the probabilities of zero for the case studies were set as 0.1, 0.3, and 0.2 for Cases 1, 2, and 3, respectively.

In the optimization of the autoregressive model weights, as shown in Figure 27, the microgrid, as shown in Figure 25, is used with random load, random wind power, and disconnection of WTG 0.10 p.u. at time 150 s. This set of data is not included in the simulation test of Cases 1 – 3 in the next subsection. The ranges of the search parameters of the autoregressive model for the estimation of RoCoF and frequency deviations are set to $[a_k^{min} \quad a_k^{max}] = [0.1 \quad 1.0]$ and $[b_k^{min} \quad b_k^{max}] = [0.1 \quad 1.0]$, respectively. The autoregressive order $p_1 = p_2 = 2$.

The parameters of the firefly algorithm were set as follows: the maximum iteration was 100, the number of fireflies was 20, the randomization parameter (α) was 0.5, the attractiveness of the firefly algorithm at iteration 0 (β_0) was 0.1, and the light absorption coefficient of the firefly (γ) was 1. Consequently, the optimal autoregressive model weights are obtained as $a_1 = 0.361$, $a_2 = 0.482$, $b_1 = 0.562$, $b_2 = 0.439$.

The efficiency of the proposed IR – MPC was compared with that of NoVESS, CMPC, and RMPC. Further details of the comparison methods are provided below:

NoVESS: Owing to the problem of DoS attacks, VESS is not included in the frequency regulation or virtual inertia control. Therefore, DoS attacks do not affect load frequency regulation or virtual inertia control.

CMPC: The VESS was controlled using conventional MPC. The effect of DoS attacks was not considered when designing the CPMC. Thus, block "Attack detector and signal estimator" is excluded from Figure 29. The DoS attack signal, as shown in Figure 40, was applied to the transmission system between the microgrid and VESS. Therefore, the effects of DoS attacks are damaged feedback signals; that is, perfect signals Δf, ΔR are changed to Δf_d, ΔR_d. The damaged signals Δf_d, ΔR_d are then fed to the CMPC controller. Consequently, the CMPC controller produces a deteriorated control signal to control the VESS during the DoS attacks.

RMPC: The VESS is controlled using a resilient MPC. In this method, during a DoS attack, the signal estimator shown in Figure 34 is designed based on the attacked current signal, which is equal to the previous signal.

Further details of the case studies are provided below.

Case 1: The system parameters were set as follows: the probability of zero of the Bernoulli binary was 0.1, $H=0.06$, $D=0.12$, and at 150s WTG disconnected 0.1 p.u. In this case, the ability of the proposed IR – MPC to handle low – level DoS attacks is investigated.

Case 2: The system parameters were set as follows: the probability of zero of the Bernoulli binary was 0.3, $H=0.06$, $D=0.12$, and at 150s the disconnection of the WTG was 0.2 p.u. In this case, the ability of the proposed IR – MPC to handle high – level DoS attacks is investigated.

Case 3: The system parameters were set as follows: the probability of zero of the Bernoulli binary was 0.2, $H=0.03$, $D=0.06$, and at 150s the WTG disconnected 0.1 p.u. A medium – level DoS attack was used. In this case, the robustness of the proposed IR – MPC to variations in the system parameters was investigated. Therefore, the microgrid inertia and damping properties were reduced by 50% in Cases 1 and 2 (i.e., $H=0.03$ and $D=0.06$) [40, 65].

The inertia constant of $H=0.03$ appeared to be excessively small. However, the problem of a zero – inertia microgrid, which consists of a 100% converter – based system, has recently been investigated [52]. Thus, the high penetration of renewable energy sources, such as WTG and PV, may reduce the inertia of the microgrid, that is, $H=0.03-0.06$, as studied in [40, 65].

The maximum RoCoF value for all simulation results in this study was 20 Hz/s [66]. The selection criteria for the maximum RoCoF settings are appropriate for explaining the simulation results. Conventionally, the maximum RoCoF settings were lower than those used in this study.

IR – MPC – based VESS Simulation Results and Discussion

The simulation results of the case studies are provided below:

Case 1: Figure 41 and 42 show the simulation results for case 1. The simulation results for Case 1 can be explained by the following three situations.

1. During normal operation (50 s – 100 s): the frequency and RoCoF deviations of the NoVESS were significantly higher than those of CMPC, RMPC, and IR – MPC. These results imply that using the VESS for virtual inertia control can reduce the frequency and RoCoF deviations, which is consistent with the simulation results of our previous study [48].

2. During DoS Attacks (100 s – 130 s): The NoVESS operates in the same manner as in normal operation because the DoS signal does not affect the VESS control, which is not used in this method. In this situation, the CMPC cannot maintain the RoCoF within an allowance limit of approximately 124s. In contrast, the RMPC and IR – MPC successfully maintained the RoCoF and frequency deviation within the allowance limit.

3. During DoS Attacks and the disconnection of the WTG (150 s – 180 s): In this situation, the proposed IR – MPC can reduce the RoCoF to a value lower than that of the RMPC and NoVESS. However, NoVESS produced a higher RoCoF than RMPC.

The simulation results for Case 1 imply that, when using the VESS for virtual inertia control, the VESS controller should be designed under a DoS attacks. If the VESS controller does not consider the effect of a DoS attacks (i.e., CMPC), the control of RoCoF and the frequency deviation will deteriorate.

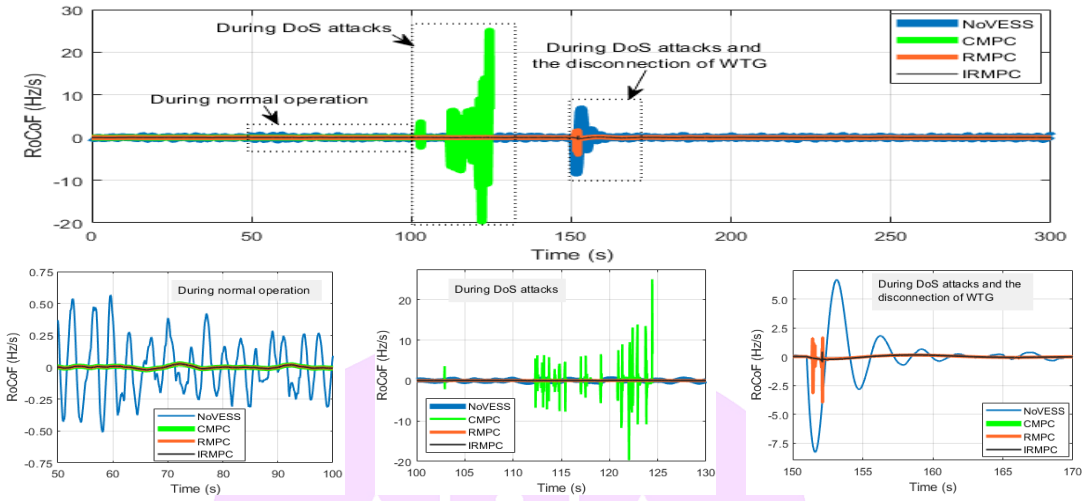


Figure 41 RoCoF of Case 1.

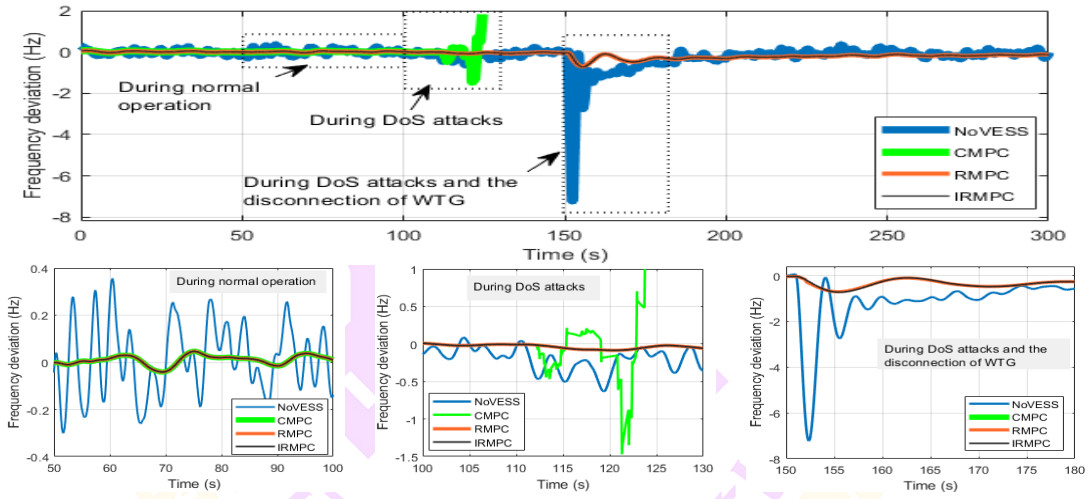


Figure 42 Frequency deviation of Case 1.

Case 2: The simulation results for Case 2 are shown in Figure 43 and 44 can be explained by the following three situations.

1. During normal operation (50 s – 100 s): the frequency and RoCoF deviations of the NoVESS were significantly higher than those of CMPC, RMPC, and IR – MPC, as in Case 1.

2. During DoS Attacks (100 s – 130 s): In this situation, the CMPC cannot maintain the RoCoF within an allowance limit of approximately 119s. In contrast, the RMPC and IR – MPC successfully maintained the RoCoF and frequency deviation within the allowance limit.

3. During DoS Attacks and disconnection of WTG (150 s – 180 s): In this situation, IR – MPC can reduce RoCoF to a value lower than that of RMPC and NoVESS. These results imply that IR – MPC can improve microgrid virtual inertia control over RMPC and NoVESS.

In this case, it can be concluded that under a high – level DoS attacks, IR – MPC can reduce the RoCoF and frequency deviation better than NoVESS, CMPC, and RMPC.

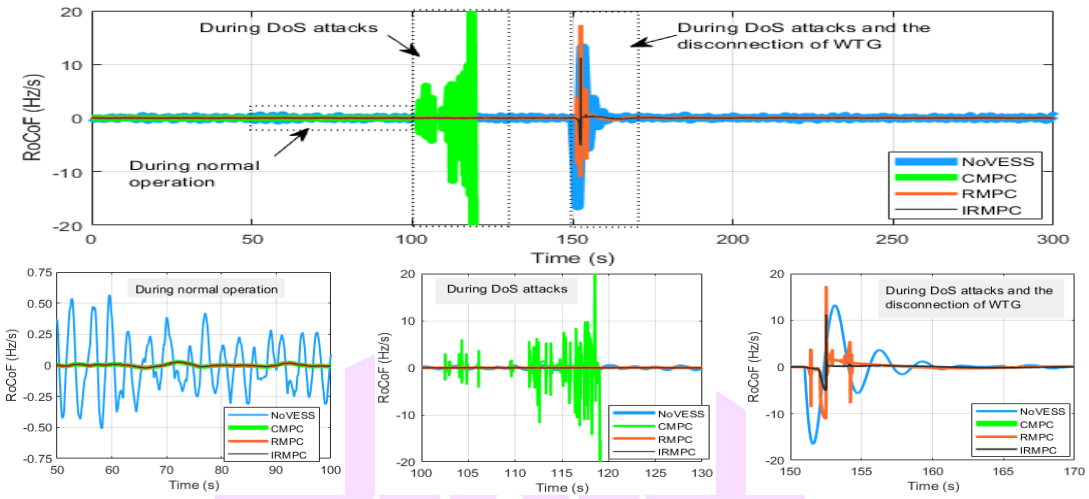


Figure 43 RoCoF of Case 2.

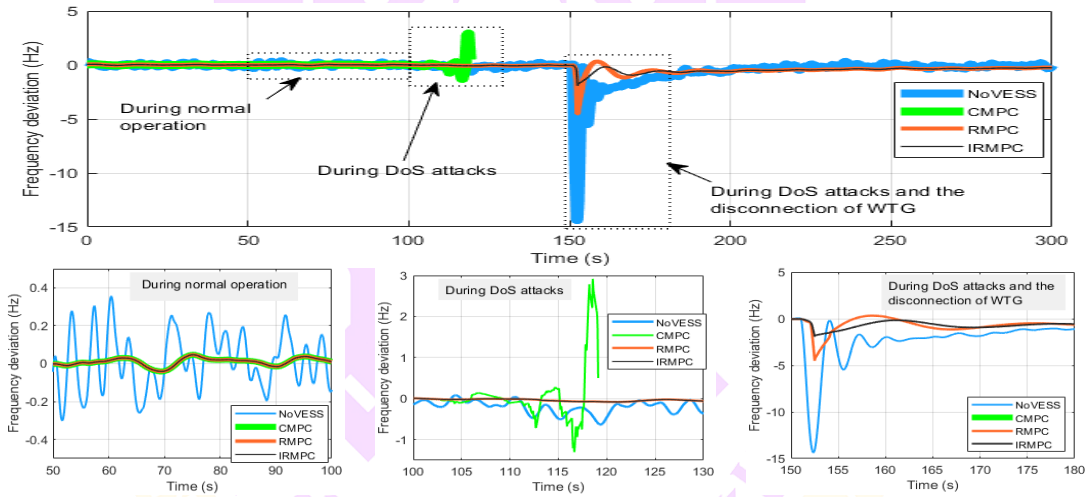


Figure 44 Frequency deviation of Case 2.

Case 3: Figure 45 and 46 show the simulation results for Case 3. The simulation results for Case 3 can be explained by the following three situations.

1. During normal operation (50 s – 100 s): the frequency and RoCoF deviations of the NoVESS were significantly higher than those of CMPC, RMPC, and IR – MPC, as in Cases 1 and 2.

2. During DoS Attacks (100 s – 120 s): In this situation, the CMPC cannot maintain the RoCoF within the maximum limit of approximately 112.5 s. In contrast, the RMPC and IR – MPC successfully maintained the RoCoF and frequency deviation within the allowance limit.

3. During DoS Attacks and disconnection of WTG (150 s – 180 s): In this situation, IR – MPC can reduce RoCoF to a value lower than that of RMPC and NoVESS. However, RMPC cannot maintain the RoCoF within an allowance limit of approximately 152s. These results imply that IR – MPC can improve microgrid virtual inertia control over RMPC and NoVESS.

In this case, it can be concluded that the proposed IR – MPC is robust to variations in the system parameters.

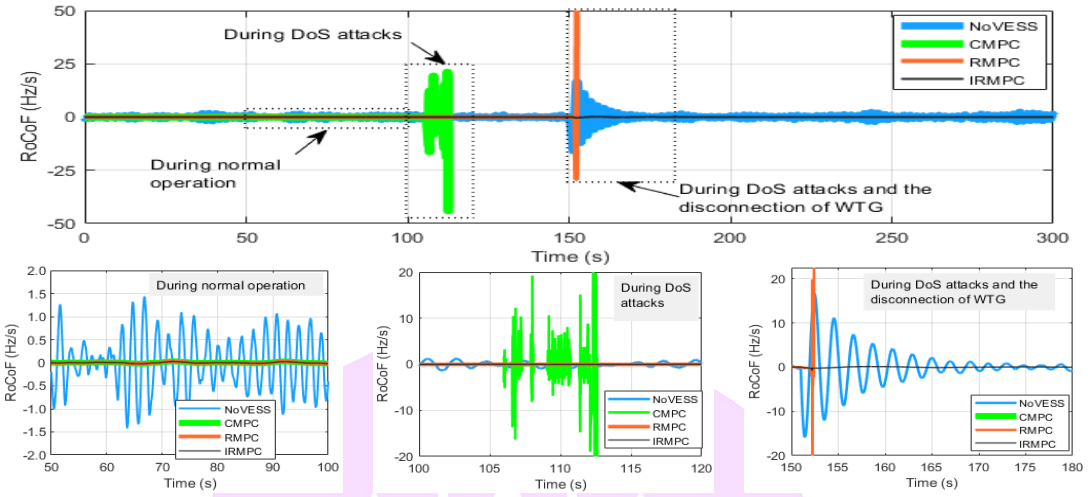


Figure 45 RoCoF of Case 3.

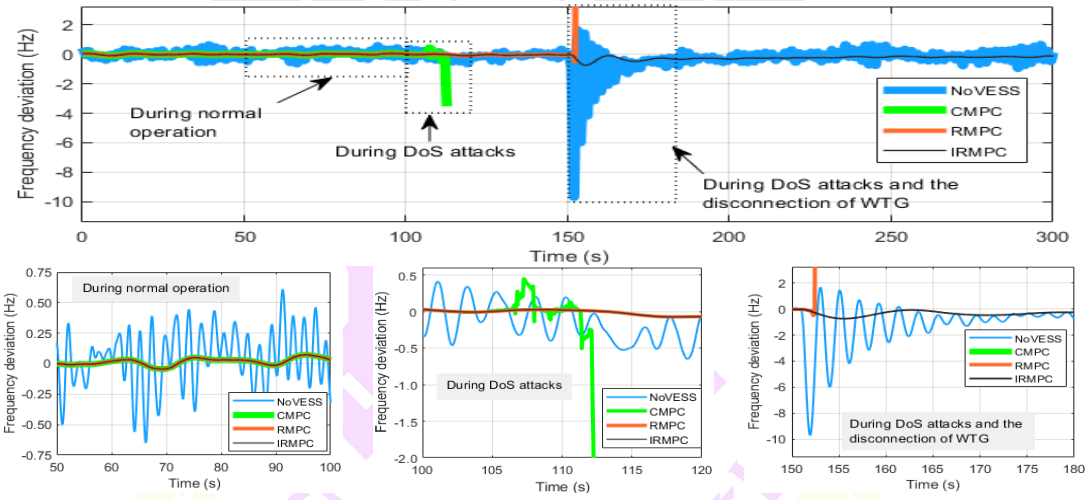


Figure 46 Frequency deviation of Case 3.

In addition, to test the proposed IR – MPC to the variation in the WTG connection/disconnection to the studied microgrid, microgrid with the parameters of Case 1 was used. Figure 47 shows the simulation results of maximum RoCoF and maximum.

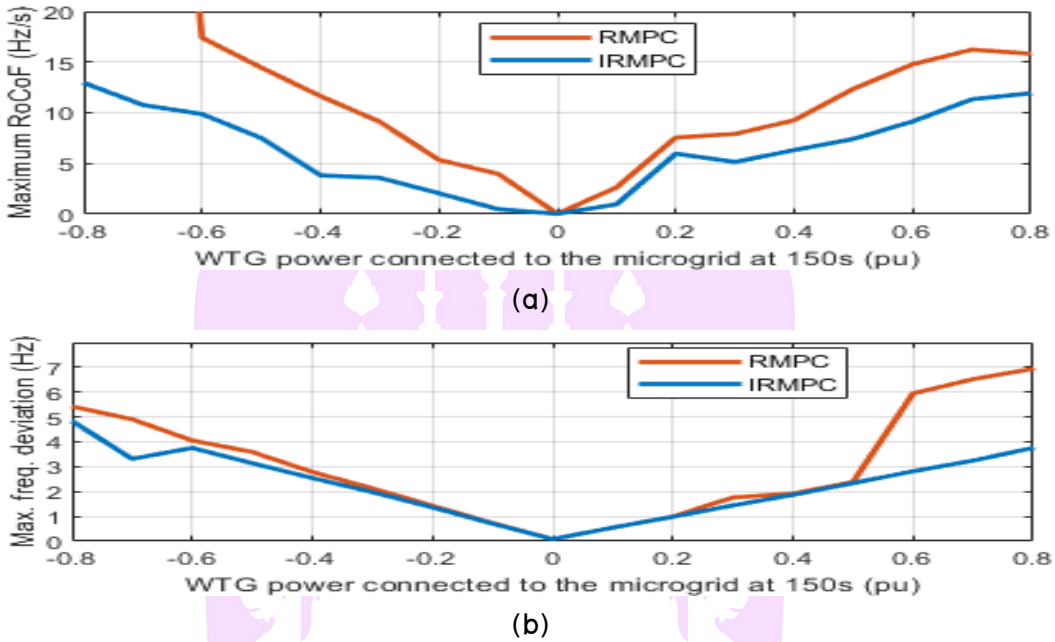


Figure 47 Simulation results when WTG connected/disconnected to the microgrid (a) maximum RoCoF (b) maximum frequency deviation.

The frequency deviation when WTG connection/disconnection to the microgrid from –0.8 p.u. to 0.8 p.u. The maximum RoCoF of IR – MPC was lower than 20 Hz/s, whereas that of RMPC was higher than 20 Hz/s when the disconnection of the WTG power was greater than 0.8 p.u. The maximum frequency deviation of RMPC and IR – MPC in Figure 47 is high during the connection/disconnection of WTG, which is allowed during contingency ($\leq \pm 5$Hz). However, the frequency deviation of the proposed IR – MPC was lower than that of the RMPC. These simulation results confirm that the proposed IR – MPC exhibits superior performance over RMPC.

PEMEL Control for Microgrid Frequency Regulations Under Severe DoS Attacks Using ER – MPC

This section presents the results of the simulation along with a discussion. First, an investigation of the impact of DoS attacks on microgrid frequency regulation using several techniques for feedback signal estimation was presented. Then, the simulation settings are described. Simulation results are presented, followed by a discussion.

Study on DoS – Attack Effects on Microgrid Frequency Regulation Using Various Methods for Estimating Feedback Signals

An autoregressive model uses historical data to forecast future events. The autoregressive model can therefore be improved to forecast frequency deviation during DoS attacks by examining the relationship between signals and DoS attacks levels.

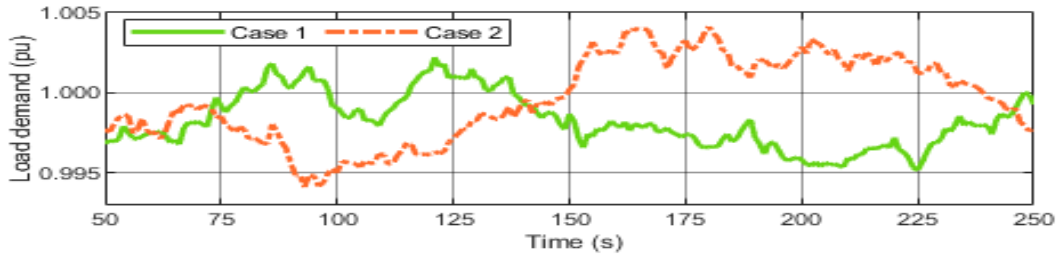
Simulation Setting

MATLAB/Simulink was used to evaluate the effectiveness of the enhanced resilient MPC (ER – MPC) for PEMEL in controlling microgrid frequency deviation under DoS attacks. The study system was a microgrid, as shown in Figure 30. Table 8 show the microgrid data [48, 60–62].

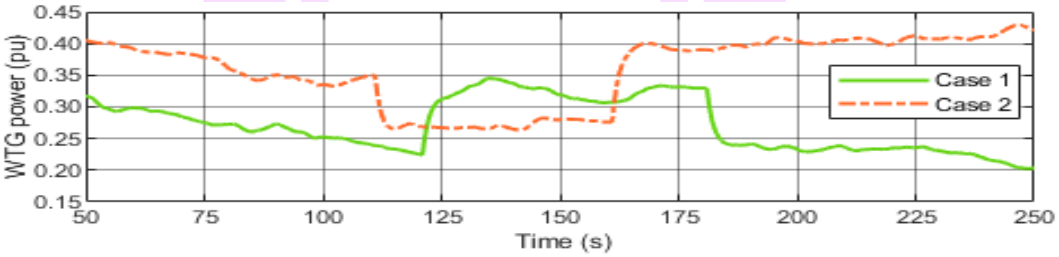
Table 8 Microgrid and PEMEL parameters values.

Parameters	Values	Parameters	Values
f_{ref}	50 Hz	P_{EL}	5 MW
H	0.06 s	K_{EL}	1.6 W/A
D	0.12 p.u.	K_{EL1}	4841.4
T_g	0.1 s	T_{EL}	37 s
T_t	0.4 s	C_d	37 F
R	2.4 (Hz/p.u.MW)	B_{H2}	0.5 m^3/s
K_i	0.2 s	B_{PEL}	82 W
		K_{H2}	0.028 m^3/As

Figure 48 shows load demand and WTG power of the case studies. The load demands of Case 1 were higher than those of Case 2 in the first simulation at 75 – 130 s. After 150 s, the load demand in Case 2 was higher than that in Case 1 for 240 s. For case 1, it is assumed that at 120 s, WTG disconnects 0.1 p.u. and reconnects 0.12 p.u. at 180 s, respectively. The stability is decreased when the WTG was disconnected. Consequently, the frequency deviation exceeds the nominal values and can reach the maximum permitted frequency.



(a)



(b)

Figure 48 Load demand and WTG power of the case studies (a) load demand (b) WTG power.

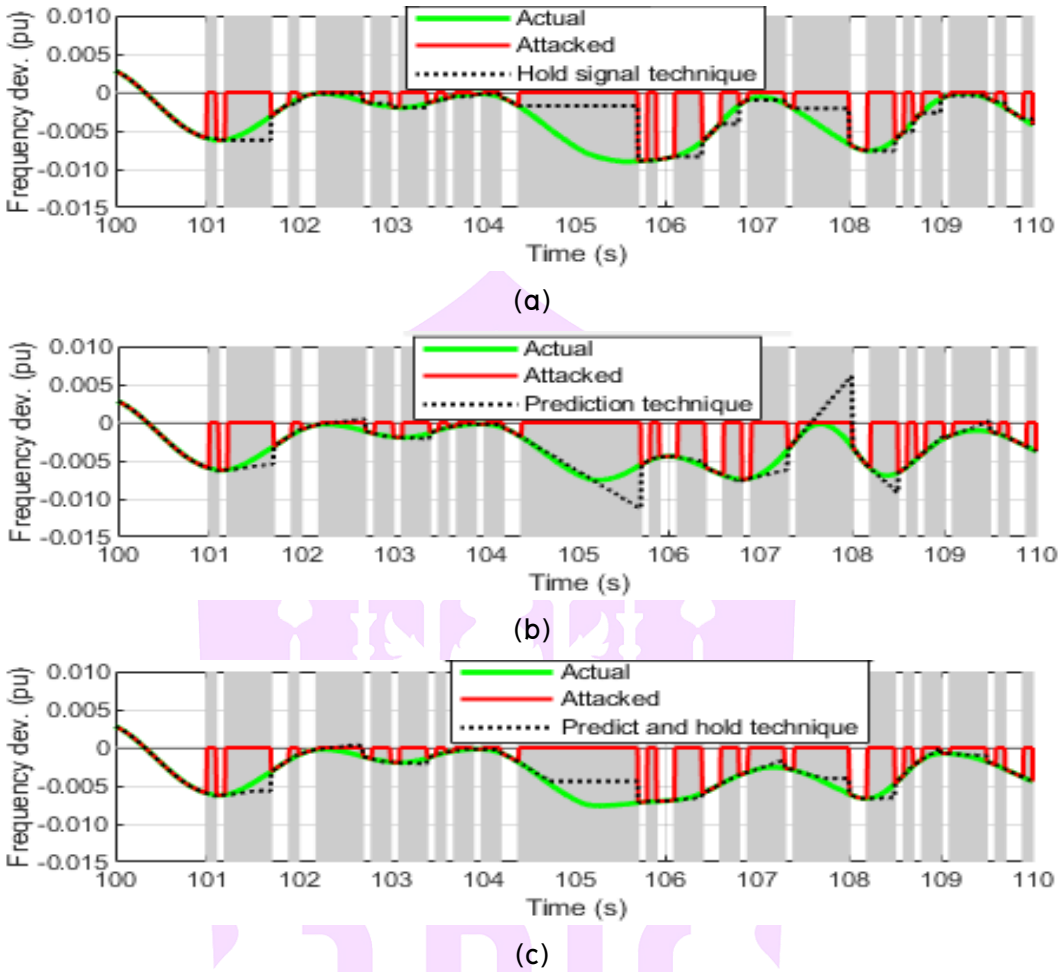


Figure 49 Frequency deviation when DoS probability of zero = 0.6

(a) hold signal (b) prediction (c) predict and hold techniques.

The efficiency of the proposed enhanced resilient model predictive control (ER – MPC) was compared with that of resilient MPC (R – MPC) and autoregressive – based resilient MPC (ARR – MPC). R – MPC was designed based on the hold signal, as shown in [67] and Figure 34 (a). The results for microgrids operated with R – MPC under normal and severe DoS attacks are shown in Figure 49 (a) and Figure 50 (a), respectively. The ARR – MPC was designed based on the hold signal and Figure 34 (b). The results for the microgrid operated with ARR – MPC under normal and severe DoS attacks are shown in Figure 51 and 52.

Figure 49 (b) and Figure 50 (b), respectively. The proposed ER – MPC was designed based on a combination of prediction and hold signals, as shown in Figure 34 (c). The results for the microgrid operated with the ER – MPC under normal and severe DoS attacks are shown in Figure 49 (c) and Figure 50 (c), respectively.

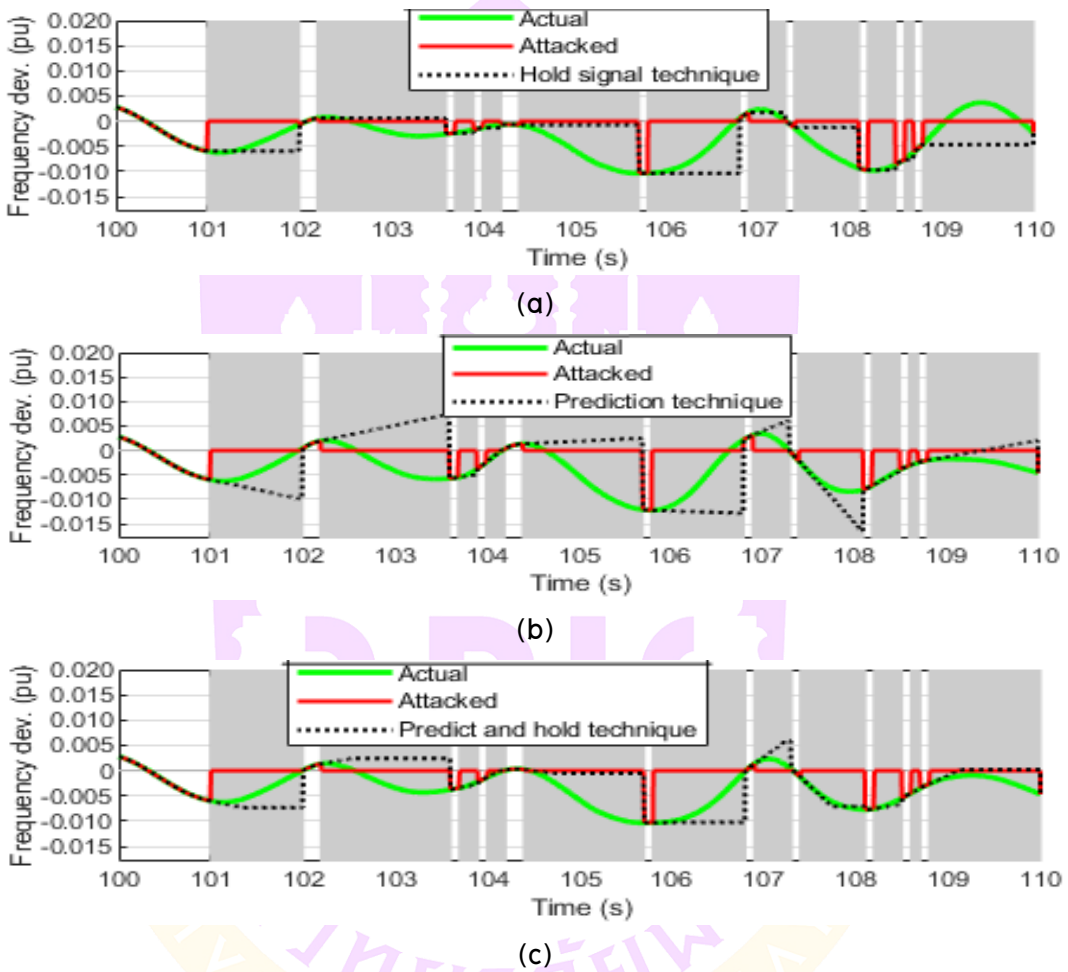


Figure 50 Frequency deviation when DoS probability of zero = 0.85

(a) hold signal (b) prediction (c) predict and hold techniques.

Simulation Results and Discussion

Figure 51 (a) – (d) show the frequency deviations of Case 1 when the DoS probabilities of zero are 0.65, 0.75, and 0.85, respectively.

Figure 51 (a) the DoS probability of zero was 0.55: the frequency deviations of R – MPC, ARR – MPC, and the proposed ER – MPC did not seem to differ.

Figure 51 (b) the DoS probability of zero was 0.65: the frequency deviations of R – MPC and ARR – MPC were slightly higher than those of ER – MPC.

Figure 51 (c) the DoS probability of zero was 0.75: the frequency deviations of R – MPC were higher than those of ARR – MPC and ER – MPC.

Figure 51 (d) the DoS probability of zero was 0.85: the frequency deviations of R – MPC and ARR – MPC are clearly higher than those of ER – MPC. The maximum frequency deviation increased when the DoS probability of zero increased.

Figure 52 displays the simulation results for Case 1 when the DoS probability is zero = 0.85.

Figure 52 (a) shows the rate of change in the frequency of the proposed and the comparison methods. The proposed ER – MPC can maintain the RoCoF of the microgrid within acceptable ranges. The R – MPC maintains the RoCoF, while the ARR – MPC deteriorates.

Figure 52 (b) shows the hydrogen production rate of the PEMEL stack.

Figure 52 (c) shows the power of the PEMEL stack. The hydrogen production rate was consistent with that of PEMEL power.

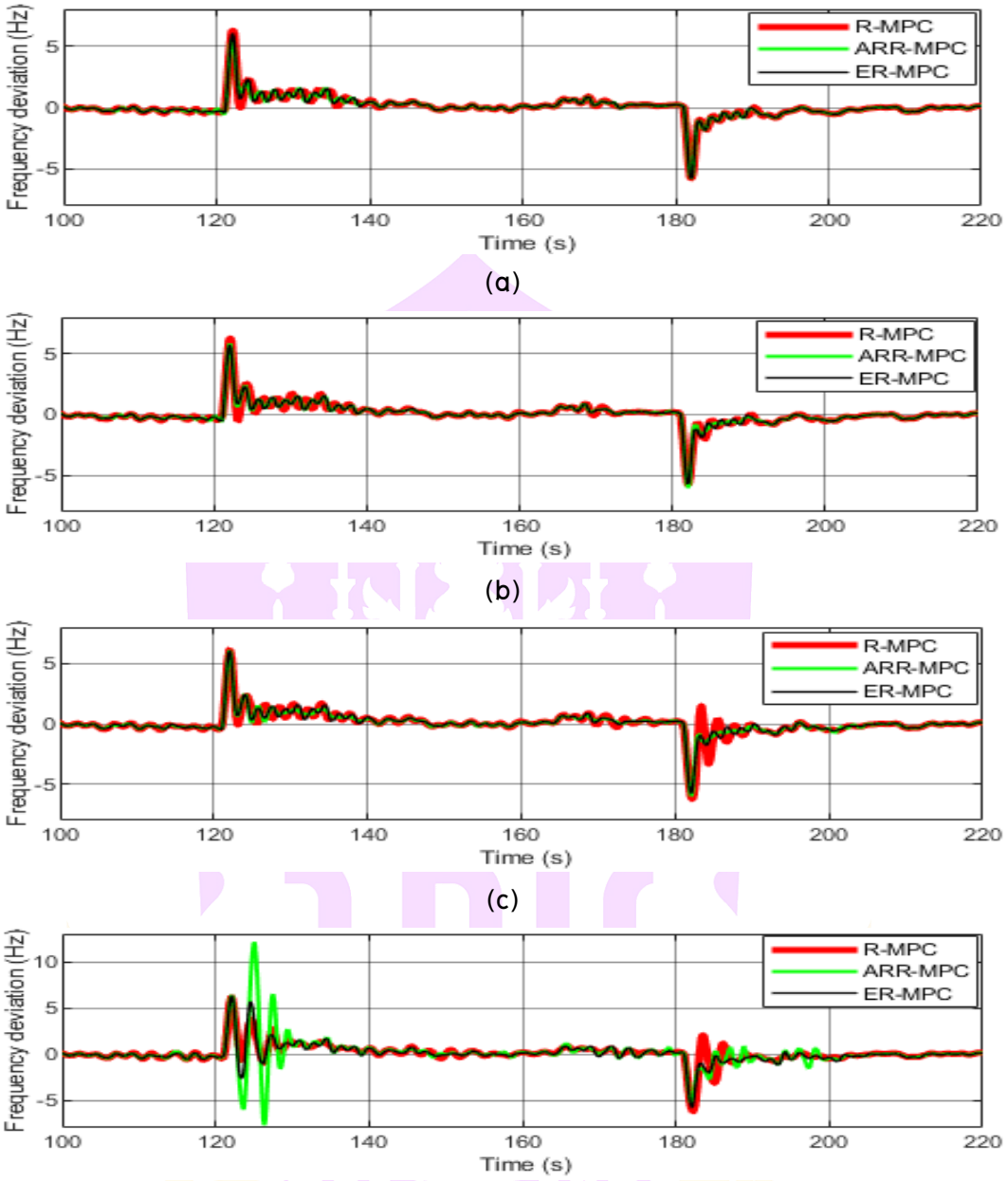


Figure 51 Frequency deviation of case 1, (a) DoS probability of zero = 0.55 (b) DoS probability of zero = 0.65 (c) DoS probability of zero = 0.75 (d) DoS probability of zero = 0.85.

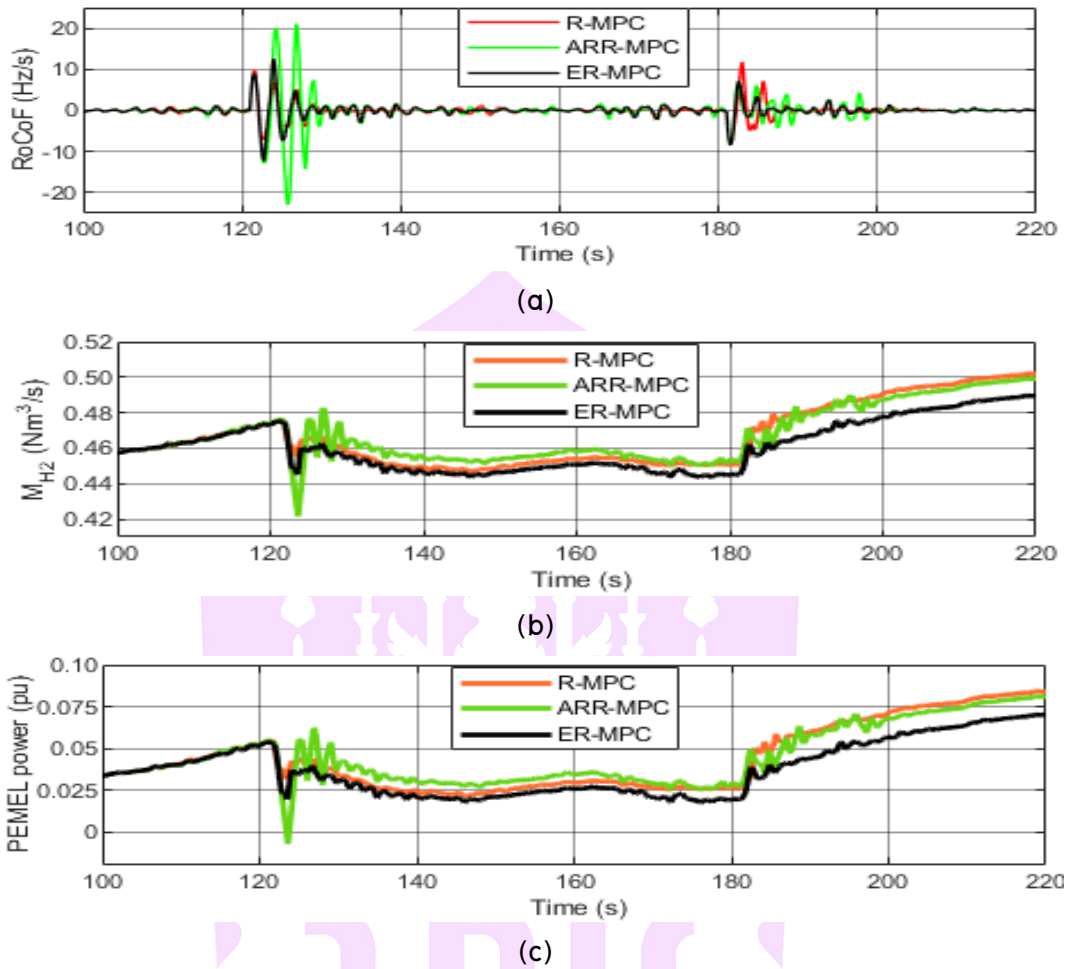


Figure 52 Simulations results of Case 1 when DoS probability of zero = 0.85 (a) RoCoF (b) hydrogen production rate (c) power of PEMEL stack.

Figure 53 (a) – (d) show the frequency deviations of Case 1 when the DoS probabilities of zero were 0.65, 0.75, and 0.85, respectively.

Figure 53 (a) the DoS probability of zero was 0.55: the frequency deviations of R – MPC, ARR – MPC, and the proposed ER – MPC did not seem to differ.

Figure 53 (b) the DoS probability is zero, is 0.65: the frequency deviations of R – MPC and ARR – MPC were slightly higher than those of ER – MPC.

Figure 53 (c) the DoS probability is zero, is 0.75: the frequency deviations of R – MPC were higher than those of ARR – MPC and ER – MPC.

Figure 53 (d) the DoS probability was zero, was 0.85: the frequency deviations of R – MPC and ARR – MPC are clearly higher than those of ER – MPC. The maximum frequency deviation increased when the DoS probability of zero increased.

Figure 54 shows the simulation results for Case 2 when the DoS probability is zero = 0.85.

Figure 54 (a) shows the rate of change in the frequency of the proposed and the comparison methods. The proposed ER – MPC can maintain the RoCoF of the microgrid within acceptable ranges. The R – MPC maintains the RoCoF, while the ARR – MPC deteriorates.

Figure 54 (b) shows the hydrogen production rate of the PEMEL stack.

Figure 54 (c) shows the power of the PEMEL stack. The hydrogen production rate was consistent with that of PEMEL power. These results confirmed that the proposed ER – MPC can improve the performance of the control method under severe DoS attacks.

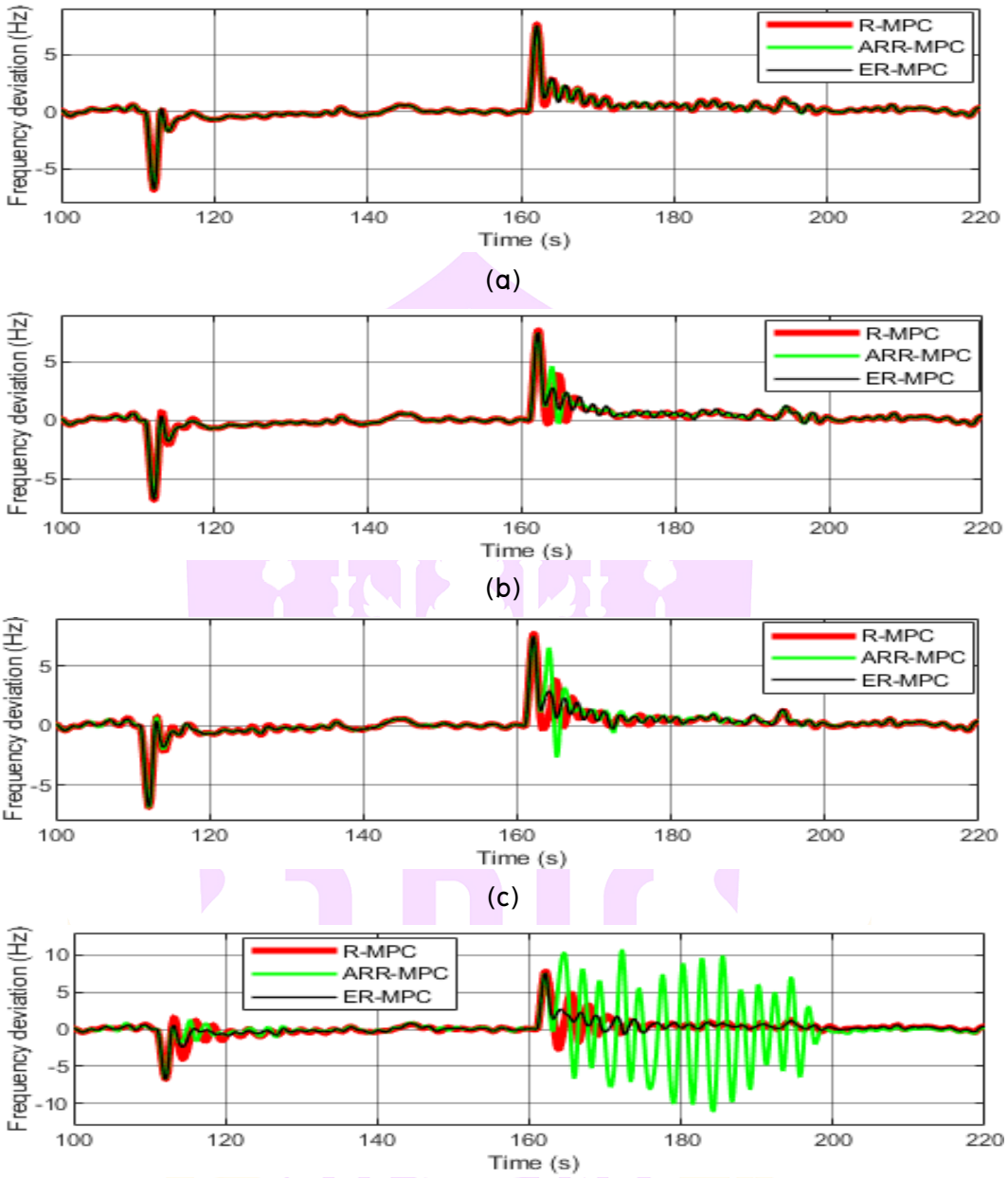
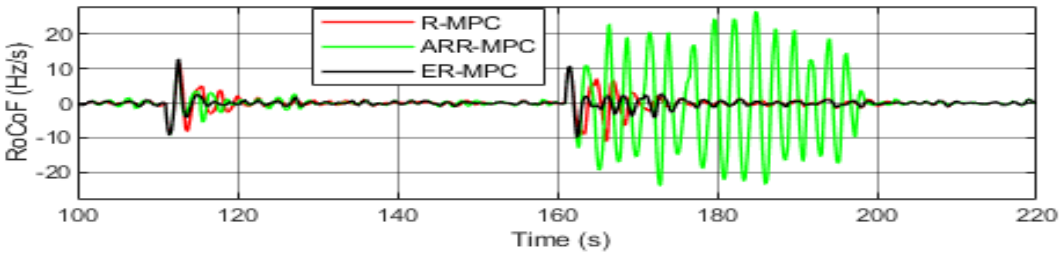
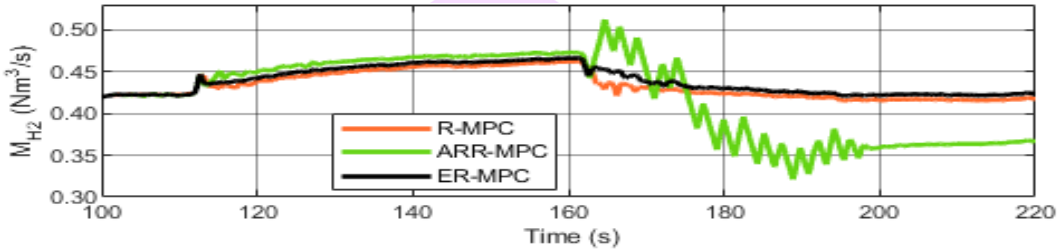


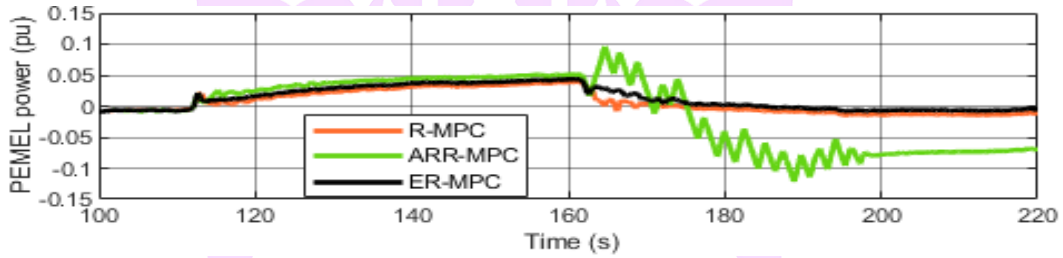
Figure 53 Frequency deviation of case 2. (a) DoS probability of zero = 0.55 (b) DoS probability of zero = 0.65 (c) DoS probability of zero = 0.75 (d) DoS probability of zero = 0.85.



(a)



(b)



(c)

Figure 54 Simulations results of Case 2 when DoS probability of zero = 0.85 (a) RoCoF (b) hydrogen production rate (c) power of PEMEL stack.

CHAPTER V

CONCLUSION

Summary of the Study

This Dissertation proposes an improved version of resilient model predictive control (R – MPC) for microgrid frequency ancillary services, that is, virtual inertia control and frequency regulation under denial of service (DoS) attacks. The conclusions of this study are as follows.

(1) An improved resilient MPC (IR – MPC) – based virtual energy storage system (VESS) for enhancing microgrid virtual inertia control under DoS attacks is explained in Chapter III. The IR – MPC uses an autoregressive (AR) – based signal estimator for reconstruction of the attacked signal feeding to R – MPC.

(2) An enhanced resilient MPC (ER – MPC) – based proton exchange membrane electrolyzers (PEMEL) to regulate frequency under severe DoS attacks is proposed in Chapter III. ER – MPC uses a combination of AR model – based prediction and hold – signal methods to reconstruct attacked signals during severe DoS attacks.

(3) The simulation results in Chapter IV reveal that under a DoS attacks, the proposed IR – MPC and ER – MPC can successfully improve the microgrid virtual inertia emulation and frequency regulation. In addition, the proposed IR – MPC and ER – MPC have a performance effect over the compared techniques in terms of the reduction in the rate of change of frequency (RoCoF) and frequency deviation during normal situations, DoS attacks, and disconnection of wind turbine generation.

Discussion of the study

1. The IR – MPC comprises an attack detector, an autoregressive (AR) signal estimator, and an MPC – based VESS controller. The AR parameters were optimized using a firefly algorithm with the objective of reducing frequency and RoCoF deviations.

2. Under a DoS attacks, the proposed IR – MPC – based VESS can successfully provide virtual inertia emulation. Furthermore, the proposed IR – MPC can reduce the rate of change of frequency (RoCoF) better than not using a VESS for virtual inertia control (No – VESS), conventional MPC – based VESS, and resilient MPC – based VESS.

3. When the microgrid inertia and damping properties are reduced, the proposed IR – MPC can maintain the RoCoF and frequency deviation within acceptable ranges, whereas the No – VESS, conventional MPC – based VESS, and resilient MPC – based VESS cannot reduce the RoCoF and frequency deviation within acceptable ranges. These results indicate that the proposed IR – MPC is robust to the microgrid parameter variations when subjected to DoS attacks.

4. The proposed ER – MPC combines autoregressive model – based prediction and holds signals for resilient model predictive control to enhance the control effect when subject to severe DoS attacks.

5. The efficacy of the suggested ER – MPC was compared with that of the autoregressive – based robust model predictive control (ARR – MPC) and resilient model predictive control (R – MPC) techniques.

6. The simulation findings, it was found that the proposed ER – MPC can effectively enhance microgrid frequency controls compared to the R – MPC and AR – MPC by lowering frequency deviation and rate of change of frequency during severe DoS attacks.

Additionally, the study results show that the combination of prediction and hold signals for resilient model predictive control is appropriate for PEMEL control of frequency regulation under severe DoS attacks.

Limitations of the Study

Recommendations for further studies that implement a model predictive control (MPC) – based Virtual Energy Storage System (VESS) for virtual inertia control and frequency regulation in a microgrid under cyberattacks pose several challenges.

1. Cybersecurity. Protecting microgrid control systems from cyberattacks is crucial. This includes securing communication networks, ensuring the integrity of control commands, and safeguarding against unauthorized access or data manipulation.

2. Accurate Modeling. Developing accurate dynamic models of microgrid components and their interactions is essential for effective MPC control. Uncertainties in model parameters or disturbances can degrade the control performance and stability.

3. Real – time Optimization. MPC requires solving optimization problems in real time to determine optimal control actions. This can be computationally intensive, particularly for large – scale microgrids with numerous distributed energy resources (DERs) and complex dynamics.

4. Adaptive Control. The control system should be adaptive to changes in microgrid operating conditions, such as variations in renewable energy generation, load fluctuations, or system topology changes owing to cyberattacks or equipment failures.

5. Integration of Renewable Energy Sources. Integrating renewable energy sources with intermittent generation patterns adds complexity to control systems. The MPC must effectively manage the variability of renewable generation while maintaining grid stability and frequency regulation.

Addressing these challenges requires interdisciplinary collaboration between power system engineers, control theorists, cybersecurity experts, and policymakers. Robust cybersecurity measures, advanced control algorithms, real – time optimization techniques, and reliable communication infrastructure are key enablers for deploying MPC – based VESS solutions in microgrids under cyberattack scenarios.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] S. S. Sami, M. Cheng, J. Wu, and N. Jenkins. (2018). A virtual energy storage system for voltage control of distribution networks. *CSEE Journal of Power and Energy Systems, 4* (2), 146 – 154. doi: 10.17775/CSEEJPES.2016.01330

[2] H. – J. r. Bullinger, C. Doetsch, and P. Bretschneider. (2012). Smart Grids – the Answer to the New Challenges of Energy Logistics?. *CESifo DICE report, 10*, 29 – 35.

[3] J. Eyer and G. Corey. (2011). Energy storage for the electricity grid: Benefits and market potential assessment guide, 1 – 232.

[4] G. N. Bathurst and G. Strbac. (2003). Value of combining energy storage and wind in short – term energy and balancing markets. *Electric Power Systems Research, 67* (1), 1 – 8. doi: https://doi.org/10.1016/S0378–7796(03)00050–6

[5] X. Luo, J. Wang, M. Dooner, and J. Clarke. (2015). Overview of current development in electrical energy storage technologies and the application potential in power system operation. Applied Energy, 137, 511 – 536. doi: https://doi.org/10.1016/j.apenergy.2014.09.081

[6] G. Strbac. (2008). Demand side management: Benefits and challenges. *Energy Policy, 36* (12), 4419 – 4426. doi: https://doi.org/10.1016/j.enpol.2008.09.030

[7] K. Samarakoon, J. Ekanayake, and N. Jenkins. (2013). Reporting Available Demand Response. *IEEE Transactions on Smart Grid, 4* (4), 1842 – 1851. doi: 10.1109/TSG.2013.2258045

[8] G. C. Heffner, C. Goldman, and B. Kirby. (2007). Loads providing ancillary services: Review of international experience.

[9] M. Behrangrad. (2015). A review of demand side management business models in the electricity market. *Renewable and Sustainable Energy Reviews, 47*, 270 – 283. doi: https://doi.org/10.1016/j.rser.2015.03.033

[10] S. Sami, M. Cheng, and J. Wu. (2016). Modelling and control of multi – type grid – scale energy storage for power system frequency response. 269 – 273.

[11] M. Cheng, S. S. Sami, and J. Wu.(2017). Benefits of using virtual energy storage system for power system frequency response. *Applied Energy, 194*, 376 – 385. doi: https://doi.org/10.1016/j.apenergy.2016.06.113.

[12] Y. He, M. Petit, and P. Dessante. (2012). Optimization of the steady voltage profile in distribution systems by coordinating the controls of distributed generations. *IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, 1 – 7. doi: 10.1109/ISGTEurope.2012.6465740

[13] H. Saberi, C. Zhang, and Z. Y. Dong. (2023). Capacity of Virtual Energy Storage System for Frequency Regulation Services via a Data – Driven Distributionally Robust Optimization Method. *IEEE Transactions on Power Systems, 38* (3), 2134 – 2147. doi: 10.1109/TPWRS.2022.3193899

[14] Y. Matsuo, A. Yanagisawa, and Y. Yamashita. (2013). A global energy outlook to 2035 with strategic considerations for Asia and Middle East energy supply and demand interdependencies. *Energy Strategy Reviews, 2* (1), 79 – 91. doi: https://doi.org/10.1016/j.esr.2013.04.002

[15] B. Kroposki et al. (2017). Achieving a 100% Renewable Grid: Operating Electric Power Systems with Extremely High Levels of Variable Renewable Energy. *IEEE Power and Energy Magazine, 15* (2), 61 – 73. doi: 10.1109/MPE.2016.2637122

[16] I. Pvps et al. (2019). Trends in photovoltaic applications.

[17] R. Yan, T. K. Saha, N. Modi, N. – A. Masood, and M. Mosadeghy. (2015). The combined effects of high penetration of wind and PV on power system frequency response. *Applied Energy, 145*, 320 – 330. doi: https://doi.org/10.1016/j.apenergy.2015.02.044

[18] J. G. Slootweg and W. L. Kling. (2002). Impacts of distributed generation on power system transient stability. *IEEE Power Engineering Society Summer Meeting, 2*, 862 – 867. doi: 10.1109/PESS.2002.1043465

[19] H. Bevrani. (2014). Robust Power System Frequency Control.

[20] H. – P. Beck and R. Hesse. (2007). Virtual synchronous machine. 1 – 6.

[21] J. Driesen and K. Visscher. (2008). Virtual synchronous generators. *IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, 1 – 3. doi: 10.1109/PES.2008.4596800

[22] Q. – C. Zhong and G. Weiss. (2011). Synchronverters: Inverters That Mimic Synchronous Generators. *IEEE Transactions on Industrial Electronics, 58*, 1259 – 1267. doi: 10.1109/TIE.2010.2048839

[23] T. Kerdphol, F. Rahman, M. Watanabe, and Y. Mitani. (2021). Virtual Inertia Synthesis for a Single – Area Power System, 61 – 90.

[24] H. Bevrani, T. Ise, and Y. Miura. (2014). Virtual synchronous generators: A survey and new perspectives. *International Journal of Electrical Power & Energy Systems, 54*, 244 – 254. doi: https://doi.org/10.1016/j.ijepes.2013.07.009

[25] U. Tamrakar, D. Shrestha, M. Maharjan, B. P. Bhattarai, T. M. Hansen, and R. Tonkoski. (2017). Virtual Inertia: Current Trends and Future Directions. *Applied Sciences, 7* (7). doi: 10.3390/app7070654

[26] M. P. N. v. Wesenbeeck, S. W. H. d. Haan, P. Varela, and K. Visscher. (2009). Grid tied converter with virtual kinetic storage. *IEEE Bucharest PowerTech*, 1 – 7. doi: 10.1109/PTC.2009.5282048

[27] P. Rodriguez, E. Rakhshani, A. Cantarellas, and D. Remon. (2015). Analysis of derivative control based virtual inertia in multi – area high – voltage direct current interconnected power systems. *IET Generation, Transmission & Distribution, 10.* doi: 10.1049/iet-gtd.2015.1110

[28] T. Kerdphol, F. Rahman, and Y. Mitani. (2018). Virtual Inertia Control Application to Enhance Frequency Stability of Interconnected Power Systems with High Renewable Energy Penetration. *Energies, 11*, 981. doi: 10.3390/en11040981

[29] D. Olivares et al. (2014). Trends in Microgrid Control. *IEEE Transactions on Smart Grid, 5*, 1905 – 1919. doi: 10.1109/TSG.2013.2295514

[30] M. Dreidy, H. Mokhlis, and S. Mekhilef. (2017). Inertia response and frequency control techniques for renewable energy sources: A review. *Renewable and Sustainable Energy Reviews, 69*, 144 – 155. doi: https://doi.org/10.1016/j.rser.2016.11.170

[31] E. Rakhshani, D. Rodriguez, A. Cantarellas, J. Martinez, and P. Rodriguez. (2017). Virtual Synchronous Power Strategy for Multiple HVDC Interconnections of Multi – Area AGC Power Systems. *IEEE Transactions on Power Systems, 32*, 1665 – 1677. doi: 10.1109/TPWRS.2016.2592971.

[32] S. D'Arco, J. Suul, and O. Fosso. (2015). A Virtual Synchronous Machine implementation for distributed control of power converters in SmartGrids. *Electric Power Systems Research, 122*. doi: 10.1016/j.epsr.2015.01.001

[33] Y. Chen, R. Hesse, D. Turschner, and H. – P. Beck. (2011). Improving the grid power quality using virtual synchronous machines, 1 – 6.

[34] H. Bevrani, B. Francois, and T. Ise. (2017). Microgrid Dynamics and Control.

[35] M. Albu, A. Nechifor, and D. Creanga. (2010). Smart storage for active distribution networks estimation and measurement solutions. *IEEE Instrumentation & Measurement Technology Conference Proceedings,* 1486 – 1491. doi: 10.1109/IMTC.2010.5488083

[36] A. Khazali, N. Rezaei, H. Saboori, and J. M. Guerrero. (2022). Using PV systems and parking lots to provide virtual inertia and frequency regulation provision in low inertia grids. *Electric Power Systems Research, 207*, 107859. doi: https://doi.org/10.1016/j.epsr.2022.107859

[37] J. M. S. D. Araujo. (2019). WRF Wind Speed Simulation and SAM Wind Energy Estimation: A Case Study in Dili Timor Leste. *IEEE Access, 7*, 35382 – 35393. doi: 10.1109/ACCESS.2019.2904755

[38] P. Kundur. (2022). Power System Stability and Control. New York,USA: McGraw Hill Education.

[39] Q. Peng, Y. Yang, T. Liu, and F. Blaabjerg. (2020). Coordination of virtual inertia control and frequency damping in PV systems for optimal frequency support. *CPSS Transactions on Power Electronics and Applications, 5* (4), 305 – 316. doi: 10.24295/CPSSTPEA.2020.00025.

[40] F. S. R. Thongchart Kerdphol, Masayuki Watanabe, Yasunori Mitani. (2021). Virtual Inertia Synthesis and Control, 1.

[41] A. Singh and Sathans. (2016). GA optimized PID controller for frequency regulation in standalone AC microgrid. *India International Conference on Power Electronics (IICPE), 7*, 1 – 5. doi: 10.1109/IICPE.2016.8079367

[42] Z. Hu, S. Liu, W. Luo, and L. Wu. (2021). Intrusion – Detector – Dependent Distributed Economic Model Predictive Control for Load Frequency Regulation With PEVs Under Cyber Attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers, 68 (9)*, 3857 – 3868. doi: 10.1109/TCSI.2021.3089770

[43] Y. Liu, Y. Li, Y. Wang, X. Zhang, H. B. Gooi, and H. Xin. (2022). Robust and Resilient Distributed Optimal Frequency Control for Microgrids Against Cyber Attacks. *IEEE Transactions on Industrial Informatics, 18* (1), 375 – 386. doi: 10.1109/TII.2021.3071753

[44] L. Kong and L. Xiao. (2007). A New Model Predictive Control Scheme – Based Load – Frequency Control. *IEEE International Conference on Control and Automation,* 2514 – 2518. doi: 10.1109/ICCA.2007.4376815

[45] J. B. Rawlings. (2000). Tutorial overview of model predictive control. *IEEE Control Systems Magazine, 20* (3), 38 – 52. doi: 10.1109/37.845037

[46] J. Pahasa and I. Ngamroo. (2016). Coordinated Control of Wind Turbine Blade Pitch Angle and PHEVs Using MPCs for Load Frequency Control of Microgrid. *IEEE Systems Journal, 10* (1), 97 – 105. doi: 10.1109/JSYST.2014.2313810

[47] S. Kayalvizhi and D. M. V. Kumar. (2017). Load Frequency Control of an Isolated Micro Grid Using Fuzzy Adaptive Model Predictive Control. *IEEE Access, 5,* 16241 – 16251. doi: 10.1109/ACCESS.2017.2735545

[48] J. Pahasa, P. Potejana, and I. Ngamroo. (2022). MPC – Based Virtual Energy Storage System Using PV and Air Conditioner to Emulate Virtual Inertia and Frequency Regulation of the Low – Inertia Microgrid. *IEEE Access, 10,* 133708 – 133719. doi: 10.1109/ACCESS.2022.3231751

[49] P. S. Tadepalli and D. Pullaguram. (2022). Distributed Control Microgrids: Cyber – Attack Models, Impacts and Remedial Strategies. *IEEE Transactions on Signal and Information Processing over Networks, 8*, 1008 – 1023. doi: 10.1109/TSIPN.2022.3230562

[50] M. Shi, X. Chen, M. Shahidehpour, Q. Zhou, and J. Wen. (2021). Observer – Based Resilient Integrated Distributed Control Against Cyberattacks on Sensors and Actuators in Islanded AC Microgrids. *IEEE Transactions on Smart Grid, 12* (3), 1953 – 1963. doi: 10.1109/TSG.2021.3050203

[51] C. Phurailatpam, Z. H. Rather, B. Bahrani, and S. Doolla. (2021). Estimation of Non – Synchronous Inertia in AC Microgrids. *IEEE Transactions on Sustainable Energy, 12* (4), 1903 – 1914. doi: 10.1109/TSTE.2021.3070678

[52] D. Obradović, M. Dijokas, G. S. Misyris, T. Weckesser, and T. V. Cutsem. (2022). Frequency Dynamics of the Northern European AC/DC Power System: A Look – Ahead Study. *IEEE Transactions on Power Systems, 37* (6), 4661 – 4672. doi: 10.1109/TPWRS.2022.3154720

[53] G. Carl, G. Kesidis, R. R. Brooks, and R. Suresh. (2006). Denial – of – service attack – detection techniques. *IEEE Internet Computing, 10* (1), 82 – 89. doi: 10.1109/MIC.2006.5

[54] S. Sahoo, Y. Yang, and F. Blaabjerg. (2021). Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks. *IEEE Transactions on Power Electronics, 36* (1), 73 – 77. doi: 10.1109/TPEL.2020.3005208

[55] S. Z. Tajalli et al. (2020). DoS – Resilient Distributed Optimal Scheduling in a Fog Supporting IIoT – Based Smart Microgrid. *IEEE Transactions on Industry Applications, 56* (3), 2968 – 2977. doi: 10.1109/TIA.2020.2979677

[56] S. Liu, P. Siano, and X. Wang. (2020). Intrusion – Detector – Dependent Frequency Regulation for Microgrids Under Denial – of – Service Attacks. *IEEE Systems Journal, 14* (2), 2593 – 2596. doi: 10.1109/JSYST.2019.2935352

[57] S. Hu, X. Ge, X. Chen, and D. Yue. (2023). Resilient Load Frequency Control of Islanded AC Microgrids Under Concurrent False Data Injection and Denial – of – Service Attacks. IEEE Transactions on Smart Grid, 14 (1), 690 – 700. doi: 10.1109/TSG.2022.3190680

[58] H. Zhu, X. You, and S. Liu. (2019). Multiple Ant Colony Optimization Based on Pearson Correlation Coefficient. *IEEE Access, 7*, 1628 – 61638. doi: 10.1109/ACCESS.2019.2915673

[59] T. Kerdphol, F. S. Rahman, Y. Mitani, M. Watanabe, and S. K. Küfeoğlu. (2018). Robust Virtual Inertia Control of an Islanded Microgrid Considering High Penetration of Renewable Energy. *IEEE Access, 6*, 625 – 636. doi: 10.1109/ACCESS.2017.2773486

[60] S. Muangchuen, J. Pahasa, and I. Ngamroo. (2023). Improved Resilient Model Predictive Control for Enhanced Microgrid Virtual Inertia Emulation by Virtual Energy Storage System Under DoS Attacks. *IEEE Access, 11*, 96817 – 96830. doi: 10.1109/ACCESS.2023.3312608

[61] M. B. Hossain, M. R. Islam, K. M. Muttaqi, D. Sutanto, and A. P. Agalgaonkar. (2023). Dynamic Electrical Circuit Modeling of a Proton Exchange Membrane Electrolyzer for Frequency Stability, Resiliency, and Sensitivity Analysis in a Power Grid. *IEEE Transactions on Industry Applications, 59* (6), 7271 – 7281. doi: 10.1109/TIA.2023.3297985.

[62] M. B. Hossain, M. R. Islam, K. M. Muttaqi, D. Sutanto, and A. P. Agalgaonkar. (2023). Power System Dynamic Performance Analysis Based on Frequency Control by Proton Exchange Membrane Electrolyzers. *IEEE Transactions on Industry Applications, 59* (4), 4998 – 5008. doi: 10.1109/TIA.2023.3257141

[63] A. R. Bemporad, N.L.; Morari, M.. (2019). Model Predictive Control Toolbox™ User's Guide; MATH WORKS Inc. Natick, MA: USA.

[64] B. Zhang, C. Dou, D. Yue, J. H. Park, and Z. Zhang. (2022). Attack – Defense Evolutionary Game Strategy for Uploading Channel in Consensus – Based Secondary Control of Islanded Microgrid Considering DoS Attack. *IEEE Transactions on Circuits and Systems I: Regular Papers, 69* (2), 821 – 834. doi: 10.1109/TCSI.2021.3120080

[65] T. Kerdphol, M. Watanabe, K. Hongesombut, and Y. Mitani. (2019). Self – Adaptive Virtual Inertia Control – Based Fuzzy Logic to Improve Frequency Stability of Microgrid With High Renewable Penetration. *IEEE Access, 7*, 76071 – 76083. doi: 10.1109/ACCESS.2019.2920886

[66] M. W. Altaf, M. T. Arif, S. Saha, S. N. Islam, M. E. Haque, and A. M. T. Oo. (2022). Effective ROCOF – Based Islanding Detection Technique for Different Types of Microgrid. *IEEE Transactions on Industry Applications, 58* (2), 1809 – 1821. doi: 10.1109/TIA.2022.3146094

[67] Q. Sun, K. Zhang, and Y. Shi. (2020). Resilient Model Predictive Control of Cyber–Physical Systems Under DoS Attacks. IEEE Transactions on Industrial Informatics, 16, (7), 4920 – 4927. doi: 10.1109/TII.2019.2963294

APPENDIX

APPENDIX A Scholarly articles

International journal article

1. S. Muangchuen, J. Pahasa, and I. Ngamroo. (2023). Improved Resilient Model Predictive Control for Enhanced Microgrid Virtual Inertia Emulation by Virtual Energy Storage System Under DoS Attacks. *IEEE Access, 11*, 96817 – 96830. doi: 10.1109/ACCESS.2023.3312608

2. S. Muangchuen, J. Pahasa, and C. Rakpenthai. (2024). Enhanced Resilient Model Predictive Control Electrolyzers for Frequency Regulations Under Severe Denial – of – Service Attacks. *IEEE Access, 12*, 65352 – 65361. doi: 10.1109/ACCESS.2024.3397874

National conference paper

1. ศตวรรษ เมืองชื่น, อิสระชัย งามหรู และ จงลักษณ์ พาหะซา. (2565). การควบคุมอินเวอร์เตอร์เครื่องปรับอากาศสำหรับเพิ่มแรงเฉื่อยเสมือนของไมโครกริด, **การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 45**, ภูสักธารรีสอร์ท อำเภอเมือง จังหวัดนครนายก, 16 – 18 พฤศจิกายน พ.ศ. 2565.

2. ศตวรรษ เมืองชื่น, วิภารัตน์ ข่มอาวุธ, เชวศักดิ์ รักเป็นไทย และจงลักษณ์ พาหะซา. (2566). การควบคุมยานยนต์ไฟฟ้าเพื่อเพิ่มแรงเฉื่อยเสมือนของไมโครกริดที่มีแรงเฉื่อยเสมือนต่ำภายใต้การโจมตีแบบปฏิเสธการให้บริการ ด้วยตัวควบคุมพีไอดีแบบยืดหยุ่น. **การประชุมวิชาการทางวิศวกรรมไฟฟ้าครั้งที่ 46**, 15 – 17 พฤศจิกายน 2566

3. ศตวรรษ เมืองชื่น และจงลักษณ์ พาหะซา. (2566). ความปลอดภัยทางไซเบอร์ของไมโครกริด. **การประชุมวิชาการพะเยาวิจัยครั้งที่ 13**, 24 – 26 มกราคม 2567

APPENDIX B Proceedings Improved Resilient Model Predictive Control for Enhanced Microgrid Virtual Inertia Emulation by Virtual Energy Storage System Under DoS Attacks

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 August 2023, accepted 3 September 2023, date of publication 6 September 2023, date of current version 12 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3312608

RESEARCH ARTICLE

Improved Resilient Model Predictive Control for Enhanced Microgrid Virtual Inertia Emulation by Virtual Energy Storage System Under DoS Attacks

SATAWAT MUANGCHUEN[1], JONGLAK PAHASA[1], (Member, IEEE), AND ISSARACHAI NGAMROO[2], (Senior Member, IEEE)

[1]Department of Electrical Engineering, School of Engineering, University of Phayao, Phayao 56000, Thailand
[2]Department of Electrical Engineering, School of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand

Corresponding author: Jonglak Pahasa (jonglak.pa@up.ac.th)

This work was supported by the National Research Council of Thailand.

ABSTRACT The distributed control of a microgrid is fully dependent on advanced information and communication technologies that are sensitive to cyber-physical systems. Cyberattacks, such as denial-of-service (DoS) attacks, can cause unstable operation of low-inertia microgrids. This paper proposes enhanced microgrid virtual inertia control under DoS attacks using an improved resilient model predictive control (IRMPC)-based virtual energy storage system (VESS). IRMPC comprises an attack detector, an autoregressive (AR)-based signal estimator, and an MPC-based VESS controller. An attack detector was used to detect the DoS attacks. An AR-based signal estimator is then used to estimate the feedback data that are subjected to DoS attacks. The firefly algorithm was used to optimize the AR parameters. The effectiveness of the proposed IRMPC was compared with that of conventional model predictive control, conventional model predictive control-based VESS, and resilient model predictive control-based VESS. The simulation results revealed that under a DoS attack, the proposed IRMPC can successfully improve the microgrid virtual inertia emulation. Additionally, the proposed IRMPC has a performance effect over the compared techniques in terms of the reduction in RoCoF deviation and frequency deviation during normal situations, DoS attacks, and disconnection of wind turbine generation. The simulation results also confirmed that IRMPC is robust to microgrid parameter variations when compared to the other methods.

INDEX TERMS Virtual inertia emulation, resilient model predictive control, DoS attacks, microgrid, virtual energy storage system.

I. INTRODUCTION

Microgrids (MGs) are small-scale power distribution systems that include local loads, control units, and distributed energy resources (DERs) [1], [2], [3]. Compared to traditional grids, MGs offer a number of benefits, including less power loss during transmission, increased local resilience, and improved operation and stability of regional electric grids [1]. Because distributed RESs such as solar and wind electricity are widely used in power systems, MGs have emerged as a promising method for successfully integrating distributed RESs [1], [2], [3]. However, distributed RESs are typically coupled to an MG through quick-response inertia-free power electronic converters, which results in a reduction in overall system inertia [4], [5], [6]. The reduction in system inertia results in frequency instability problems in microgrids [1], [2].

Typically, energy storage systems (ESS) are used to maintain the power imbalance in a microgrid caused by the intermittent generation of RESs [2], [3]. Additionally, the high rate of change of frequency (RoCoF) during contingencies has been reduced by using ESSs to simulate the virtual inertia of an MG [6]. Nevertheless, events that cause high RoCoF are less frequent in power systems [6] and

The associate editor coordinating the review of this manuscript and approving it for publication was Youngjin Kim.

the investment costs of ESS are high [7]. Therefore, it is not economically feasible to employ an ESS in a virtual inertial emulator.

Virtual energy storage systems (VESS) have been developed to address the high investment costs of ESS [8], [9]. A VESS can be utilized for virtual inertia control [7], load frequency control [8], and other ancillary services for power systems.

On the other side, it is well established that distribution control in microgrids is scalable and reliable [1], [2], [3]. Information exchange among DERs typically occurs through sensing and communication systems [1], [2], [3]. Owing to their heavy reliance on communication networks, microgrids are susceptible to cyberattacks. Cyberattacks such as denial of service (DoS) and false data injection (FDI) attacks have been studied for the distributed control of microgrids [10], [11]. By accessing and altering the exchange of information, FDI attacks may compromise the microgrid's data integrity [10]. DoS attacks interrupt communication services, which hampers system functioning [10], [11].

Various methods have been proposed to enhance the distributed control of microgrids subjected to cyberattacks, including fallback control [12], resilient even-triggered control [11], [13], and resilient control [10], [14], [15], [16], [17]. Shi et al. [10] investigated observer-based resilient frequency controls against cyberattacks that occur in sensors and actuators. Resilient distributed optimal scheduling control under DoS attacks was proposed in [14]. Liu et al. [15] examined how the frequency regulation changed in response to DoS attacks. Hu et al. [16] proposed resilient load-frequency management for simultaneous DoS and FDI attacks. However, the resilient controllers in [10], [14], [15], and [16] were designed based on the estimation of a microgrid state-space model. The estimation of the state-space during DoS attacks may deteriorate when a signal used to provide the state-space were subjected to cyberattacks.

Model predictive control (MPC), an adaptive optimal control technique, was recently developed to enhance the performance of multiple control objectives [18]. MPC calculates the control signal by minimizing the cost function for a constrained dynamical system over a predictable receding horizon [18]. With encouraging results, MPC can be used for frequency regulation and virtual inertia control [7]. In addition, an improved MPC was introduced to mitigate cyberattacks, such as data driven MPC [19] and resilient MPC (RMPC) [20], [21]. The RMPC in [20] combined a control law based on optimization and a control law from state feedback to implement a dual-mode MPC strategy. The RMPC in [21] uses a restricted cyber-physical system that is vulnerable to significant attacks on its communication links. A study on an aircraft model concluded that attack detection and system control could be performed remotely.

However, the RMPC in [20] held a control signal during cyberattacks that was similar to that before cyberattacks. Nevertheless, holding control signals for long periods may deteriorate the control capability. Thus, a simple prediction of control signals during cyberattacks is important. Various methods can be used for short-time signal prediction with different success levels, such as the data-driven approach [22], modified unbiased finite impulse response estimator [23], adjacent prediction [17], [24], and autoregressive (AR) prediction [25], [26]. The adjacent prediction in [17] and [24] uses signals from neighboring measurements instead of attack data, which is appropriate for an attack on a sensor. The AR models in [25] and [26] appear to be appropriate for predicting short-term control signals during DoS attacks, because the AR method is simple to implement and uses a short period of stored data. Nevertheless, AR parameter tuning is important for producing effective control actions during a DoS attack.

In addition, emulation inertia control under DoS attacks was proposed in [27]. In [7], we proposed a model predictive control for virtual inertia emulation using a VESS. However, we did not consider the effects of cyberattacks. Therefore, this study aims to investigate an MPC-based VESS for microgrid virtual inertia control under a DoS attack. An improved resilient MPC (IRMPC) is introduced to mitigate the effectiveness of DoS attacks. An autoregressive model prediction was used to estimate the attacked signals. The autoregressive parameters were optimized using the firefly algorithm [28]. The primary contributions of this study are as follows:

(1) We propose an improved resilient MPC-based VESS control technique for virtual inertia and frequency regulation under DoS attacks that has not been studied in the literature.

(2) We propose a new control technique that reduces the effect of DoS attacks by predicting the attacked data from the stored data before sending them to MPCs.

(3) The proposed improved resilient MPC-based VESS control method can be used with various levels of success by DoS attackers and variations in the system parameters.

The remainder of this paper is organized as follows. The formulation of the problem and system modeling are discussed in Section II. Section III provides details of the improved resilient MPC-based VESS for virtual inertia control against DoS attacks. The simulation results and related discussions are presented in Section IV. Section V concludes the paper.

II. PROBLEM FORMULATION AND MODELING OF THE SYSTEM

The problem formulation and modeling of the system are presented in this section. First, virtual inertia emulation of the power system is introduced. Next, the microgrid control under a DoS attack is introduced. Subsequently, a linearized microgrid for virtual inertia control and denial-of-service attacks was described. Finally, the capacity of the VESS from the inverter air conditioner and photovoltaic generators was clarified.

A. MICROGRID CONTROL UNDER DoS ATTACK

In the distribution control of a microgrid, the controller is placed close to distributed elements such as wind turbine

generators, photovoltaic generators, inverter air conditioners, and virtual energy storage systems [3]. The dynamic performance of the microgrid can be significantly enhanced by the signals sent from the sensors to the distributed controller. Nevertheless, cyberattacks are widespread in communication networks and significantly affect the microgrid stability, operation, and control.

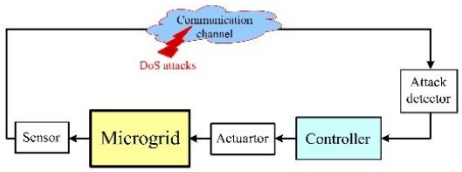


FIGURE 1. Microgrid control under DoS attacks.

Figure 1 shows the distributed microgrid control under denial-of-service attacks. DoS attacks were applied in the transmission channel between the "Sensor" and "Controller" blocks. DoS attacks damage system operations by disabling communication services [10]. The performance of the controllers may deteriorate during the DoS attacks. In this manner, the "Controller" should be designed to mitigate the effect of DoS attack to the control actions. In this study, an improved resilient model predictive control (IRMPC) is proposed to improve the performance of control actions. The "Attack detector" block is included to detect the DoS attack of the cyber-physical system.

B. INTRODUCTION TO POWER SYSTEM'S VIRTUAL INERTIA EMULATION

A typical power system inertia is the rotating mass of synchronous generators synchronously connected to a power system network. The speed of the rotating mass changes when the demand exceeds the supply at any given instant. The increasing number of renewable-based distributed generators connected to power system networks via inertia-less power electronic inverters causes a reduction in power system inertia. The emulation of virtual inertia from an inverter is a promising choice to increase the inertia of renewable-based modern power systems [5]. In addition, smart loads, such as smart air conditioners connected to the grid via inverters, can be applied for virtual inertia emulation [7].

As explained in [5], a power electronic inverter was used to emulate the swing equation of the synchronous generator to implement a virtual inertia control. The following is an expression for the synchronous generator swing equation:

$$\bar{P}_m - \bar{P}_e = \frac{2H}{\omega_0}\frac{d^2\delta}{dt^2} = \frac{2H}{\omega_0}\frac{d\Delta\omega_r}{dt} \tag{1}$$

where $\bar{P}_m$ and $\bar{P}_e$ are the mechanical and electrical powers of the synchronous generator, respectively. H denotes the inertia constant. ω_0 and ω_r denote the rated angular and angular velocities of the rotor, respectively. δ is the rotor angle, and t is the time. When the damping component with the damping coefficient K_D is included, Eq. (1) becomes.

$$\bar{P}_m - \bar{P}_e = \frac{2H}{\omega_0}\frac{d\Delta\omega_r}{dt} + K_D\frac{\Delta\omega_r}{\omega_0} \tag{2}$$

For load frequency control problems, the angular velocity deviation ($\Delta\omega_r$) was changed to the frequency deviation (Δf). Thus, Eq. (2) can be represented as:

$$\bar{P}_m - \bar{P}_e = \frac{2H}{f_0}\frac{d\Delta f}{dt} + K_D\frac{\Delta f}{f_0} \tag{3}$$

where f_0 and f are the rated and instantaneous frequencies of the power system, respectively. $d\Delta f/dt$ is the power system rate of change of frequency or RoCoF.

C. MICROGRID MODEL FOR VIRTUAL INERTIA CONTROL

Virtual inertia is described as inertial support from distributed non-synchronous generation, energy storage devices, or smart loads that mimic the inertial response of a traditional power plant using an appropriate control technique and a power electronic interface [33].

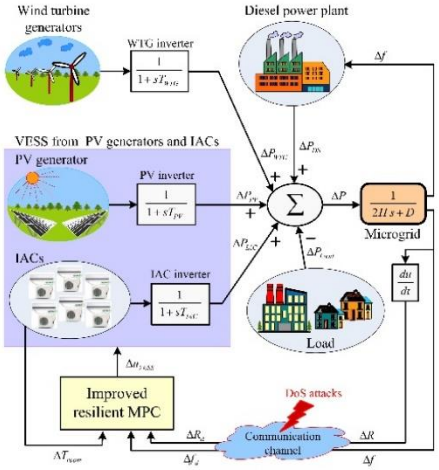


FIGURE 2. Microgrid with the proposed IRMPC for virtual inertia control using VESS from PV generator and IACs under DoS attacks.

Figure 2 shows the microgrid model for the virtual inertia control employed in this study. The microgrid consists of a diesel power plant (DS), wind turbine generators (WTG), photovoltaic generators (PV), inverter air conditioners (IACs), and traditional loads. The major source of microgrid inertia comes from the synchronous machine representation with the governor and rotor inertia of diesel power plants. The WTG, PV, and IACs are connected to the microgrid via a power electronic converter, which conventionally has low- and zero-inertia [34]. Furthermore, neither inertia controllers nor damping controllers were installed on any of the power

generators. As a result, wind and PV power generation significantly alters the operating point of the microgrid and decreases the inertia and damping characteristics of the system. Thus, the stability and performance of the microgrid are reduced. To solve this problem, a virtual energy storage system (VESS) was used to supply the microgrid with virtual inertia and frequency regulation services. A VESS is a combination of PV power generation and inverter air conditioners.

As shown in Fig. 2, the difference between the generated power and the load demand causes a change in the nominal system frequency. If the generated power is less than the load, then the speed and frequency of the generator units begin to decrease. If the generated power exceeds the load, then the speed and frequency of the generators begin to increase. The microgrid frequency deviation (Δf) can be obtained as:

$$\Delta f = \frac{1}{2H\,s + D} \times \left(\underbrace{\Delta P_{DS} + \Delta P_{PV} + \Delta P_{WTG}}_{\text{generated power}} \quad \underbrace{-\Delta P_{Load} - \Delta P_{IAC}}_{\text{demanded power}} \right) \tag{4}$$

where H and D are the inertial and damping properties of the microgrid, respectively. ΔP_{DS} is the power deviation of the diesel generator. ΔP_{PV} is the power deviation of photovoltaic generators. ΔP_{WTG} is the power deviation of the wind turbine generators. ΔP_{Load} is the power deviation of the load demand. ΔP_{IAC} is the power deviation of the inverter air conditioner.

The rate of change of frequency or RoCoF of the microgrid can be defined as

$$R = \frac{d\,\Delta f}{dt} = \frac{\Delta f(t) - \Delta f(t_p)}{t - t_p}, \quad t > t_p \tag{5}$$

where R is a short symbol of RoCoF. t and t_p represent the current and previous simulation times, respectively. $\Delta f(t)$ and $\Delta f(t_p)$ are the frequency deviations at the current time, t and the previous time t_p, respectively.

In this study, IRMPC was used to control a virtual energy storage system (VESS) derived from inverter air conditioners and photovoltaic generators to emulate virtual inertia under DoS attacks. The objectives of the IRMPC controller are as follows:

1) To improve the virtual inertia emulator.

2) To regulate the frequency deviation.

3) To control the indoor temperature, the main objective of the IACs.

4) Mitigating the effect of DoS attacks on virtual inertia and frequency-regulation controllers.

Note: As shown in Fig. 2, we assume that the diesel power plant is located near the control center. The frequency deviation (Δf) is transmitted to a diesel power plant through a short transmission line. Frequency control of diesel power plants may not consider the effects of DoS attacks. Therefore, this study did not consider the effects of DoS attacks on the control of diesel power plants.

D. DENIAL OF SERVICE ATTACK MODELING

One of the most serious security concerns to cyber-physical systems is denial of service (DoS) attacks [29]. To occupy or use limited resources, DoS attacks send misleading and meaningless data to power system components [10], [16], [24]. The DoS attack event timing is indicated by:

$$\Im(0, \infty) \triangleq \bigcup_{l \in \mathbb{N}} [T_{on,l},\ T_{off,l}] \tag{6}$$

where T denotes the sampling period, $T_{on,l} \in [T_{on}^{\min}, T]$, $l \in \mathbb{N}$ denotes the time at which a DoS attack first occurs, and $T_{off,l} \in [T_{off}^{\min}, T]$, $l \in \mathbb{N}$ indicates the moment when the DoS attack is over. The trigger time for each DoS attack was $T_{on} < T_{off} \leq T$, and the attack duration was $T_{off} - T_{on}$.

The model of a nonperiodic random variable DoS attack during all activation times can be defined as:

$$S_{DoS}(t) = \begin{cases} 0, & t \in \Im(0, \infty) \\ 1, & t \notin \Im(0, \infty) \end{cases} \tag{7}$$

where $S = 0$ denotes the occurrence of DoS attacks and $S = 1$ denotes normal transmission.

The detection of DoS attacks is an important procedure in cyber-physical systems. DoS attack detection methods can be placed locally to protect a potential victim, or remotely to detect spreading attacks [29].

In this study, attack detection was performed locally near the IRMPC-based VESS controller. We assumed that attack detection can detect attacks with promising results. DoS attacks can be detected using the method described in [29]. In addition, the RoCoF and frequency signals were sent from the microgrid sensor through the communication channel to the distributed IRMPC-based VESS controller. Thus, RoCoF and frequency deviations are transmitted under DoS attacks. Consequently, the RoCoF and frequency deviations should be predicted to improve the effectiveness of the model predictive controller. Therefore, in the next subsection, the autoregressive (AR) models used to predict RoCoF and frequency signals during DoS attacks are explained.

E. VIRTUAL ENERGY STORAGE SYSTEM MODEL

Owing to the high cost of typical energy storage systems, a virtual energy storage system (VESS) was used to improve the virtual inertia control under DoS attacks. A VESS integrates multiple electrical parts that can be controlled, including distributed generators, flexible loads, and energy storage devices [8]. A VESS can charge or discharge power to smoothen the power output variations of renewable generation [8], reduce frequency deviations, and provide virtual inertial control [7].

In this study, the VESS from inverter-air conditioners and photovoltaic generators is used to provide virtual inertia control and frequency regulation using an IRMCP controller.

The inverter-air conditioners and photovoltaic generators are combined and used as the VESS because the capacity of inverter-air conditioners and photovoltaic generators can support virtual inertia during the entire day, that is, during the night by IACs and during the day by IAC and PV.

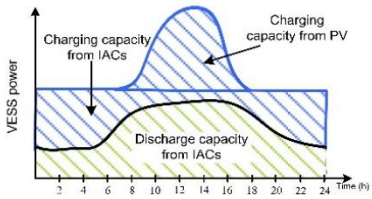


FIGURE 3. Capacity of virtual energy storage system from inverter air conditioner and photovoltaic generator.

Figure 3 shows the total VESS capacities of the IACs and photovoltaic generators. The PV system generates power during the day, discharges power during the day, and cannot support a virtual inertial emulator at night. The IAC consumes low power during the night and high power during the day. The IAC has a very low charging capacity during the day, which may not support a virtual-inertia emulator. Thus, the capacity of the VESS from the IACs and photovoltaic generator was adequate to sustain the virtual inertial emulator throughout the day.

III. PROPOSED IMPROVED RESILIENT MODEL PREDICTIVE CONTROL FOR VIRTUAL INERTIA EMULATION BY VESS UNDER DOS ATTACKS

This section presents the proposed IRMPC for virtual inertia emulation using a VESS under DoS attacks. First, we explain the autoregressive model-based prediction of RoCoF and frequency deviations during DoS attacks. Next, the correlation coefficients of the time series prediction data are presented. Consequently, the autoregressive model weight tuning is described. Finally, an IRMPC for virtual inertia emulation using a virtual energy storage system was explained.

A. AUTOREGRESSIVE MODEL-BASED PREDICTION OF ROCOF AND FREQUENCY DEVIATIONS

Autoregressive (AR) models are conventional statistical techniques that can be used to predict time-series data [25], [26]. The current output of an AR stochastic process is linearly dependent on past outputs. The definition of an AR model of order p is given by:

$$x_t = \sum_{k=1}^{p} h_k x_{t-k} + \varepsilon_t \tag{8}$$

where $x_t \in \mathbb{R}$ is the autoregressive model output; h_k is the autoregressive coefficient for the k^{th} lag; integer t denotes a time step; and $\varepsilon_t \in \mathbb{R}$ is the noise of the process, which is often assumed to be a zero-mean Gaussian variable with a finite variance σ^2.

The memory length of the autoregressive model p was captured by its order. The number of prior outputs on which the current output depends is measured by the memory length, p. The expected value of x_t can be defined as:

$$\tilde{x}_t = \sum_{k=1}^{p} h_k x_{t-k} \tag{9}$$

which along with σ^2 parameterizes the predictive distribution of $\{x_t\} \sim N(\tilde{x}_t, \sigma^2)$ conditional on the p previous measurement.

In this study, the AR model was used to predict the RoCoF deviation (ΔR) and frequency deviation (Δf) feedback signals during a DoS attack.

The AR model for predicting the RoCoF deviation can be expressed as

$$\Delta\tilde{R}(t) = \sum_{k=1}^{p_1} a_k \Delta R_d(t-k) \tag{10}$$

where $\Delta\tilde{R}(t)$ is the predicted RoCoF deviation at time t, p_1 is the order of the AR model for the prediction of RoCoF deviation, and a_k is the weight of the AR models for predicting the RoCoF deviation. ΔR_d is the RoCoF deviation, which is transmitted through the communication link and is damaged by the DoS attack.

The AR model for prediction frequency deviation can be defined as:

$$\Delta\tilde{f}(t) = \sum_{k=1}^{p_2} b_k \Delta f_d(t-k) \tag{11}$$

where $\Delta\tilde{f}(t)$ is the predicted frequency deviation at time t, p_2 is the order of the AR model for predicting frequency deviation, and b_k is the weight of the AR model for predicting frequency deviation. Δf_d is the frequency deviation transmitted through the communication link that is damaged by DoS attacks.

B. CORRELATION COEFFICIENT OF THE TIME SERIES PREDICTON DATA

The correlation coefficient is a statistical concept that helps establish a relationship between the predicted and actual values obtained in a statistical experiment [26], [30]. The calculated value of the correlation coefficient explained the difference between the predicted and actual values. The correlation coefficient value always lies between -1 and $+1$. If the correlation coefficient is positive, then there is a similar and identical relationship between the two variables.

The correlation coefficient of the two random variables is a measure of their linear dependence. If each variable has N scalar observations, the Pearson correlation coefficient is defined as

$$\rho(A,B) = \frac{1}{N-1} \sum_{i=1}^{N} \left(\frac{A_i - \mu_A}{\sigma_A}\right)\left(\frac{B_i - \mu_B}{\sigma_B}\right) \tag{12}$$

where μ_A and σ_A are the mean and standard deviation of variable A, respectively, and μ_B and σ_B are the mean and standard deviation of variable B, respectively. Alternatively, the correlation coefficient in terms of the covariance of A and B can be defined as

$$\rho(A, B) = \frac{cov(A, B)}{\sigma_A \sigma_B} \tag{13}$$

In this study, the correlation coefficient was used to calculate the relationship between the current signal and the delay signal. This correlation coefficient can be used to select the order p of the AR models.

C. AUTOREGRESSIVE MODEL WEIGHT TUNING

The autoregressive model weights (a_k and b_k) for the prediction of the RoCoF and frequency deviations were tuned simultaneously using a firefly algorithm (FLA) [28]. The objective function is the summation of the integral absolute error (IAE) of the frequency deviation [31] and the RoCoF deviation. Thus, the objective function can be expressed as

$$\begin{aligned} &\text{Minimize IAE} = \int_{t_s}^{t_e} |\Delta f|\, dt + \int_{t_s}^{t_e} |\Delta R|\, dt, \\ &\text{Subject to} \quad a_{k,\min} \le a_k \le a_{k,\max}, \\ &\qquad\qquad b_{k,\min} \le b_k \le b_{k,\max}, \quad k = 1, 2, \ldots, p. \end{aligned} \tag{14}$$

where t_s and t_e are the start and end times of the simulations, respectively. $a_{k,\min}$ and $a_{k,\max}$ are the minimum and maximum weights of the AR models, respectively, for predicting the RoCoF deviation. $b_{k,\min}$ and $b_{k,\max}$ are the minimum and maximum weights of the AR models for predicting the frequency deviation, respectively, and k is the number of AR models used.

The procedure for the autoregressive model weight tuning using the firefly algorithm is shown in Fig. 4, where γ is the light absorption coefficient of the firefly, α is the randomization parameter, and β_0 is the attractiveness of the firefly algorithm at iteration 0 [28].

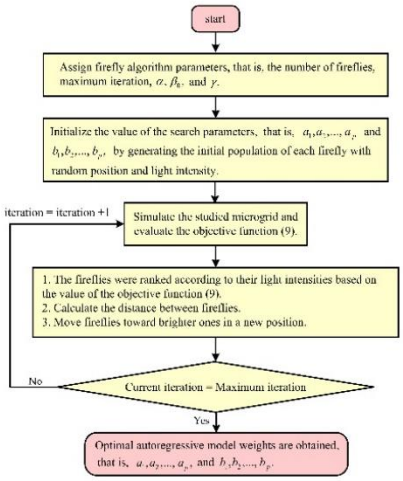


FIGURE 4. The autoregressive model weight tuning using firefly algorithm.

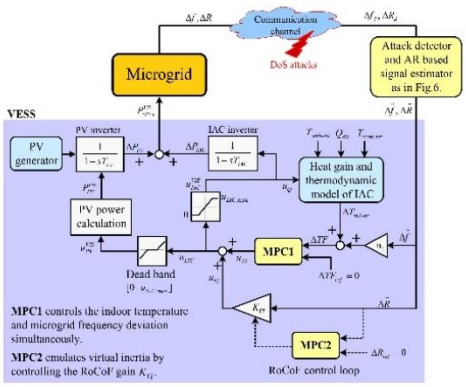


FIGURE 5. Proposed improved resilient model predictive control for virtual inertia emulation by virtual energy storage system under DoS attacks.

D. THE IMPROVED RESILIENT MODEL PREDICTIVE CONTROL FOR VIRTUAL INERTIA EMULATION BY VESS

MPC is an adaptive optimal control method that optimizes the control signal at each time instant. Resilient MPC (RMPC) was proposed in [17] and [18] to mitigate the MPC control effect during cyberattack. The proposed improved resilient model predictive control (IRMPC) for virtual inertia emulation by virtual energy storage system under DoS attack is illustrated in Fig. 5. The IRMPC based VESS controller comprises MPC1 and MPC2.

MPC1 was used to simultaneously control indoor temperature deviation (ΔT_{indoor}) and regulate microgrid frequency deviation ($\Delta \tilde{f}$). Consequently, the sum of the room temperature deviation and weighted frequency deviation served as MPC1's input, that is, ($\Delta T_{indoor} + w_1 \Delta \tilde{f}$). The selection of the frequency weight w_1 is important because the minimal and maximal temperature deviations, and the minimal and maximal frequency deviations are affected by the frequency weight w_1. The main idea is to increase the frequency deviation in the range of puThis work uses $w_1 = 100$.

MPC2 was used to control the virtual inertia of the microgrid by controlling the initial gain of VESS (K_{VI}). The RoCoF deviation ($\Delta \tilde{R}$) was used as the input, whereas K_{VI} was used as the output of MPC2.

When a DoS attack occurs, the frequency and RoCoF deviations deteriorate, and the ability of the conventional MPC-based VESS to control virtual inertia weakens.

Consequently, this study proposes an improved resilient MPC-based VESS for virtual inertia emulation, as illustrated in Fig. 5. The block "Attack detector and signal estimator" is included in the preprocessing of the frequency deviation signal before sending it to the MPCs.

Additionally, the control signals of conventional resilient control methods are predicted or held during cyberattacks [10], [14], [15], [16]. However, owing to the multi-objective control of the MPC-based VESS, the predicted control signal (Δu_{VESS}) cannot be used during the DoS attack. The VESS control signal was calculated using the indoor temperature, microgrid frequency deviation, and RoCoF deviation as the input of the IRMPC controller.

The indoor temperature is a local signal measured near the IRMCP controller and not sent through the communication link. DoS attacks do not deteriorate the indoor temperature signals. Thus, the original indoor temperature signal can be used as input to the IRMPC during DoS attacks.

In contrast, the microgrid frequency deviation and RoCoF deviation are sent from the microgrid control center through the communication link. Therefore, a DoS attack deteriorates the microgrid frequency deviation and the RoCoF deviation signals. Consequently, the attack detector and signal estimator were applied to predict the microgrid frequency and RoCoF deviation signals during DoS attacks.

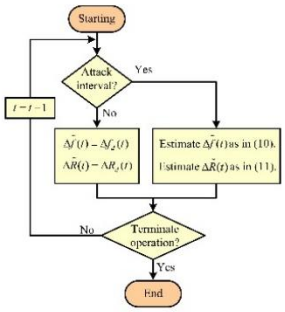


FIGURE 6. Attack detector and autoregressive model-based signal estimator.

Figure 6 shows the attack detector and autoregressive model-based signal estimator, which are used to predict the microgrid frequency deviation and RoCoF deviation signals during the DoS attacks.

IV. SIMULATION RESULTS AND DISCUSSION

The simulation results and discussion are presented in this section. First, the study of RoCoF and frequency deviation signals versus time delays is described, and then the simulation settings are explained. Subsequently, the simulation results and a discussion are presented.

A. STUDY ROCOF AND FREQUENCY DEVIATION SIGNALS VERSUS TIME DELAYS

The autoregressive model predicts the future based on previous data. Thus, the study of RoCoF and frequency deviation signals versus time delays can help the autoregressive model effectively predict RoCoF and frequency deviation during DoS attacks.

Figure 7 shows the relationship between the current RoCoF and the delay RoCoF in sub-figures A, B, and C. The upper sub-figure in Fig. 7 shows the time-domain simulation of the RoCoF, in which the positions of sub-figures A, B, and C are located. Sub-figure A shows the scatter plot of the current RoCoF and the delay RoCoF for approximately 150s, and the RoCoF between -7.5 and -6.0 Hz/s. The delays considered were 0, 1, 2, 3, and 4. Delay = 0 indicates that the current signal is plotted against the current signal (the same signal). Therefore, the data are represented by black lines. This is an ideal case for a regression problem. However, in the prediction signal during a DoS attack, the signal with a delay = 0 is unknown. We know the past signals at delays = 1, 2, 3,4 and etc. Thus, the relationship between these delay signals and the current signal was studied. For the signal with delay = 1 versus delay = 0 (green dotted line), the signal is spread closer to the black line than the signal with delays = 2, 3, and 4. These details imply that signal with delay = 1 can predict signal with delay = 0, which is better than the others. Moreover, when the delay time increased, the scatter plot spread out of the black line. The scatter plots in sub-figure A, B, and C demonstrate that the signal with time delays = 1 and 2 are appropriate for use in the linear regression of the AR model of RoCoF prediction.

Figure 8 shows the relationship between the frequency deviation and delay frequency deviation in the three sub-figures A, B, and C. The upper figure in Fig. 8 shows the time-domain simulation of the frequency deviation, in which the positions of sub-figures A, B, and C are located. The scatter plot in sub-figures A, B, and C demonstrates that a signal with time delays = 1 and 2 are appropriate for use in the linear regression of the AR model of frequency deviation prediction.

TABLE 1. Correlation coefficient of delay RoCoF versus RoCoF with delay 0.

	Time of measured (s)						
Delay	0-150	150-160	160-170	170-180	180-190	190-200	200-300
0	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1	0.9997	0.9998	0.9997	0.9997	0.9998	0.9996	0.9997
2	0.9989	0.9991	0.9989	0.9989	0.9992	0.9986	0.9990
3	0.9976	0.9979	0.9976	0.9976	0.9981	0.9968	0.9977
4	0.9958	0.9964	0.9957	0.9958	0.9967	0.9944	0.9959

Table 1 shows the correlation coefficients of the RoCoF signal with time delays = 0, 1, 2, 3, and 4, against that of time delay = 0. The RoCoF signal with delay = 0 against

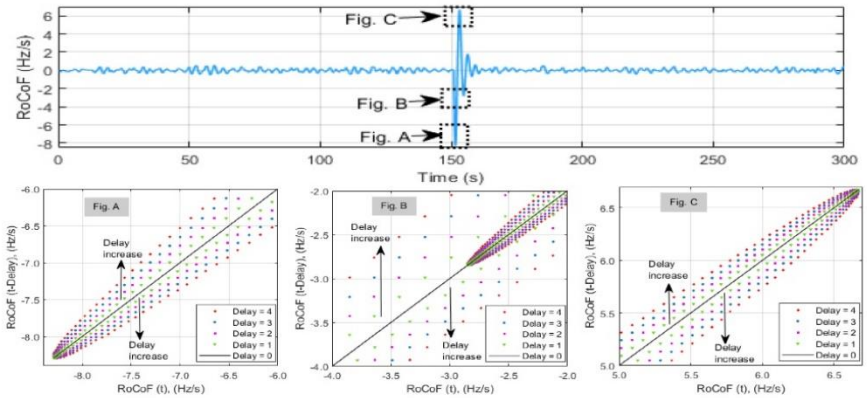


FIGURE 7. The relationship between current RoCoF ($RoCoF(t)$) and time delay RoCoF ($RoCoF(t - Delay)$).

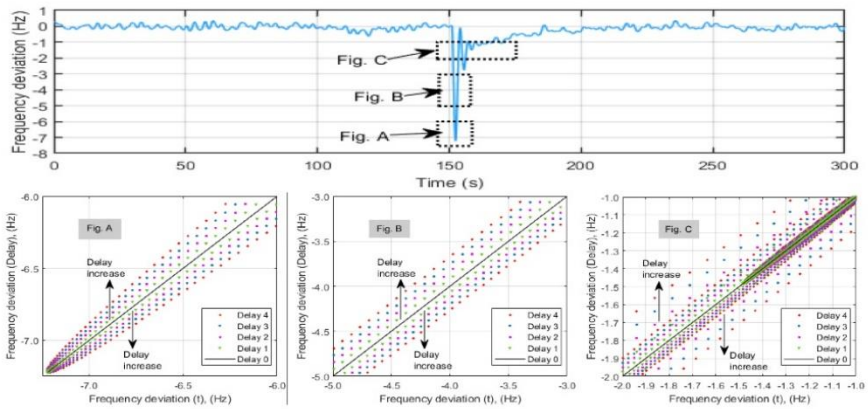


FIGURE 8. The relationship between current frequency deviation ($\Delta f(t)$) and time delay frequency deviation ($\Delta f(t - Delay)$).

the RoCoF signal with delay = 0 (the same signal) has a correlation coefficient = 1. A correlation coefficient = 1 indicates perfect regression, which is consistent with Fig. 7. When the RoCoF signal with delay = 1, the correlation coefficient near 1 appears to be a near perfect regression. However, during the disconnection of the WTG at 150-200s, the correlation coefficient was lower than that of under normal operation at 0-150s and 200-300s. The correlation coefficients clearly decreased when the delay was greater than 3. Thus, signals with delays = 1 and 2 have a correlation coefficient close to that of delay = 0. Therefore, the AR model $p = 2$ is appropriate for the RoCoF prediction.

Table 2 shows the correlation coefficients of the frequency deviation signal with time delays = 0, 1, 2, 3, and 4, against that of time delay = 0. The frequency deviation signal with delay = 0 against the frequency deviation signal with delay = 0 (the same signal) has a correlation coefficient = 1. A correlation coefficient = 1 indicates perfect regression,

TABLE 2. Correlation coefficient of delay Δf versus Δf with delay 0.

	Time of measured (s)						
Delay	0-150	150-160	160-170	170-180	180-190	190-200	200-300
0	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
1	0.9999	0.9999	0.9999	1.0000	0.9999	0.9999	0.9999
2	0.9997	0.9995	0.9996	0.9999	0.9998	0.9996	0.9996
3	0.9993	0.9988	0.9991	0.9997	0.9995	0.9991	0.9992
4	0.9988	0.9979	0.9984	0.9995	0.9991	0.9984	0.9986

which is consistent with Fig. 8. When the frequency deviation signal with delay = 1, the correlation coefficient near 1 appears to be a near perfect regression. However, during the disconnection of the WTG at 150-200s, the correlation coefficient was lower than that of under normal operation at 0-150s and 200-300s. The correlation coefficients clearly decreased when the delay was greater than 3. Thus, signals with delays = 1 and 2 have a correlation coefficient close to that of delay = 0. Therefore, the AR model $p = 2$ is appropriate for the frequency deviation prediction.

B. SIMULATION SETTING

The efficiency of the proposed IRMPC for improving microgrid virtual inertia when subjected to denial-of-service attacks was assessed using MATLAB/Simulink. The MATLAB/Simulink MPC toolbox was used to perform MPC [18]. The microgrid, shown in Fig. 2, was used as the study system. The microgrid data were obtained from [7].

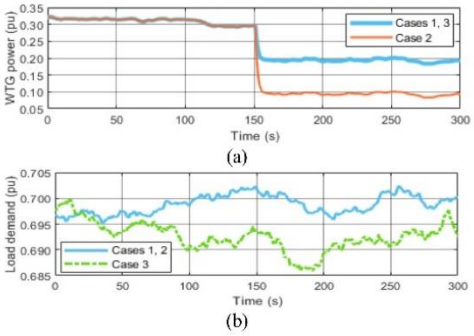


FIGURE 9. WTG power and load demand of the case studies (a) WTG power (b) load demand.

Figure 9 (a) shows the wind turbine generation (WTG) for the case studies. It is assumed that at 150 s, WTG disconnects 0.1 pu, 0.2 pu, and 0.1 pu for Cases 1, 2, and 3, respectively. The disconnection of the WTG causes a reduction in the inertia of the microgrid. Thus, the RoCoF is higher than the nominal value and may reach the RoCoF maximum allowance limit. The load demands of the case studies are shown in Fig. 9 (b). The load demands of Cases 1 and 2 were higher than that of Case 3. However, the oscillation of the load demand in Case 3 was higher than those in Cases 1 and 2. The higher oscillation of the load demand in Case 3 can cause the frequency and RoCoF deviations to be higher than in Cases 1 and 2.

Figure 10 shows the DoS attack signals used in the case studies. The Bernoulli random variable was used to generate the DoS signals [24]. When using the MATLAB/Simulink toolbox, the DoS attack level can be changed by varying the probability of zero for a Bernoulli random variable. A probability of zero implies a probability of DoS attacks

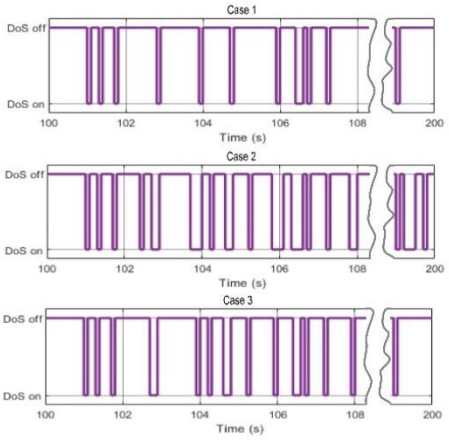


FIGURE 10. DoS attack signal of the case studies.

in the transmission system. If the probability of zero is zero, this implies that there are no DoS attacks on the transmission system. If the probability of zero is one, this implies that many DoS attacks occur in the transmission system and none of the signals can be transmitted through the transmission link. In this study, the probabilities of zero for the case studies were set as 0.1, 0.3, and 0.2 for Cases 1, 2, and 3, respectively.

In the optimization of the autoregressive model weights, as shown in Fig. 4, the microgrid, as shown in Fig. 2, is used with random load, random wind power, and disconnection of WTG 0.10 pu at time 150 s. This set of data is not included in the simulation test of Cases 1-3 in the next sub-section. The ranges of the search parameters of the autoregressive model for the estimation of RoCoF and frequency deviations are set to $[a_k^{\min} \ a_k^{\max}] = [0.1 \ \ 1.0]$ and $[b_k^{\min} \ b_k^{\max}] = [0.1 \ \ 1.0]$, respectively. The autoregressive order $p_1 = p_2 = 2$.

Parameters of the firefly algorithm were set as follows: the maximum iteration was 100, the number of fireflies was 20, the randomization parameter (α) was 0.5, the attractiveness of the firefly algorithm at iteration 0 (β_0) was 0.1, and the light absorption coefficient of the firefly (γ) was 1. Consequently, the optimal autoregressive model weights are obtained as

$$a_1 = 0.361, \ a_2 = 0.482, \ b_1 = 0.562, \ b_2 = 0.439.$$

The efficiency of the proposed IRMPC was compared with that of NoVESS, CMPC, and RMPC. Further details of the comparison methods are provided below:

NoVESS: Owing to the problem of DoS attacks, VESS is not included in frequency regulation or virtual inertia control. Therefore, DoS attacks do not affect load frequency regulation or virtual inertia control.

CMPC: The VESS is controlled using conventional MPC. The effect of DoS attacks was not considered when

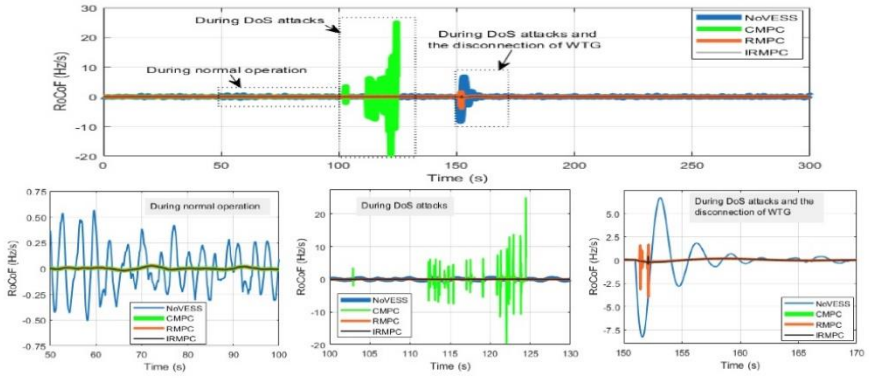


FIGURE 11. RoCoF of Case 1.

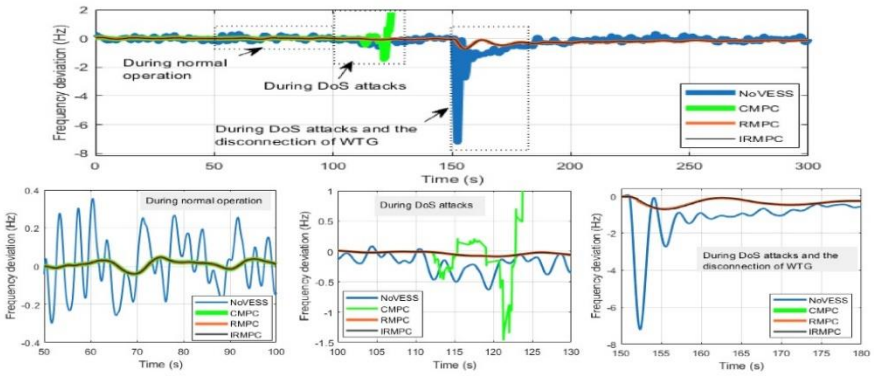


FIGURE 12. Frequency deviation of Case 1.

designing the CPMC. Thus, block "Attack detector and signal estimator" is excluded from Fig. 6. The DoS attack signal, as shown in Fig. 10, is applied to the transmission system between the microgrid and VESS. Therefore, the effects of DoS attacks are damaged feedback signals, that is, perfect signals Δf, ΔR are changed to Δf_d, ΔR_d. The damaged signals Δf_d, ΔR_d are then fed to the CMPC controller. Consequently, the CMPC controller produces a deteriorated control signal to control the VESS during the DoS attacks.

RMPC: The VESS was controlled using a resilient MPC. In this method, during a DoS attack, the signal estimator shown in Fig. 6 is designed on the basis of the attacked current signal, which is equal to the previous signal.

Further details of the case studies are provided below.

Case 1: The system parameters were set as follows: the probability of zero of the Bernoulli binary was 0.1, $H = 0.06$, $D = 0.12$, and at 150s WTG disconnected 0.1 pu. In this case, the ability of the proposed IRMPC to handle low-level DoS attacks is investigated.

Case 2: The system parameters were set as follows: the probability of zero of the Bernoulli binary was 0.3, $H = 0.06$, $D = 0.12$, and at 150s the disconnection of the WTG was 0.2 pu. In this case, the ability of the proposed IRMPC to handle high-level DoS attacks is investigated.

Case 3: The system parameters were set as follows: the probability of zero of the Bernoulli binary was 0.2, $H = 0.03, D = 0.06$, and at 150s the WTG disconnected 0.1 pu. A medium-level DoS attack was used. In this case, the robustness of the proposed IRMPC to variations in the system parameters was investigated. Therefore, the microgrid inertia and damping properties were reduced by 50% in Cases 1 and 2 (i.e., $H = 0.03$ and $D = 0.06$) [5], [35].

The considered inertia constant of $H = 0.03$ seems to be excessively small. However, the problem of a zero-inertia

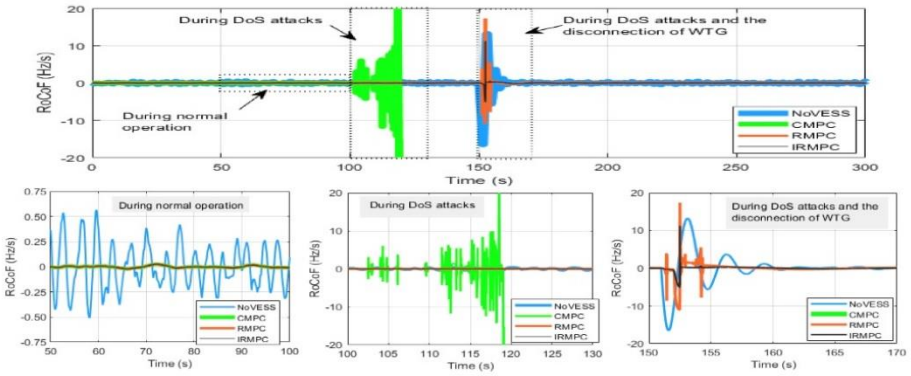


FIGURE 13. RoCoF of Case 2.

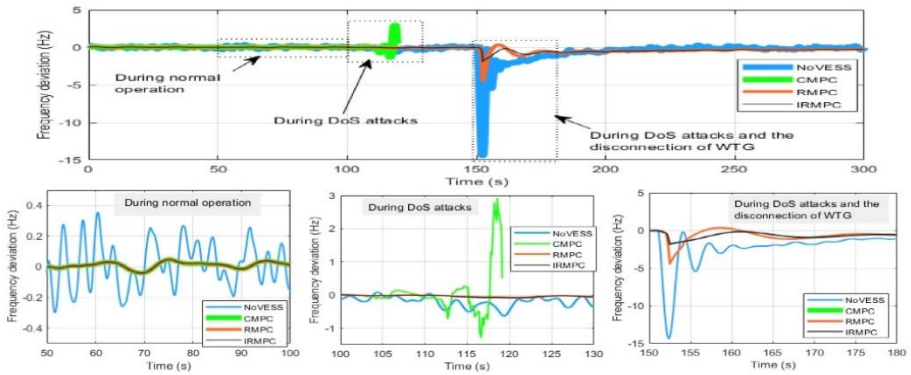


FIGURE 14. Frequency deviation of Case 2.

microgrid, which consists of a 100% converter-based system, has recently been investigated [34]. Thus, the high penetration of renewable energy sources, such as WTG and PV, may reduce the inertia of the microgrid, that is, $H = 0.03 - 0.06$, as studied in [5], and [35].

Note: The maximum RoCoF value for all simulation results in this study was 20 Hz/s [32]. The selection criteria for the maximum RoCoF settings are appropriate for explaining the simulation results. Conventionally, the maximum RoCoF settings were lower than those used in this study.

C. SIMULATION RESULTS AND DISCUSSION

The simulation results of the case studies are provided below.

Case 1: Figs. 11 and 12 show the simulation results for Case 1. The simulation results for Case 1 can be explained by the following three situations.

1.1) During normal operation (50s-100s): The frequency and RoCoF deviations of the NoVESS were significantly higher than those of the CMPC, RMPC, and IRMPC. These results imply that using VESS for virtual inertia control can reduce the frequency and RoCoF deviations, which is consistent with the simulation results of our previous study [7].

1.2) During DoS attacks (100s-130s): The NoVESS operates in the same manner as in normal operation, because the DoS signal does not affect the VESS control, which is not used in this method. In this situation, the CMPC could not maintain the RoCoF within an allowance limit of approximately 124s. In contrast, RMPC and IRMPC can successfully maintain the RoCoF and frequency deviation within the allowance limit.

1.3) During DoS attacks and the disconnection of WTG (150s-180s): In this situation, the proposed IRMPC can

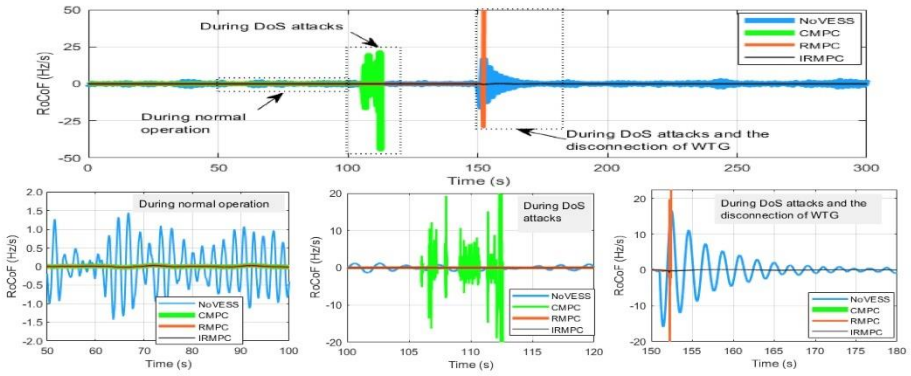


FIGURE 15. RoCoF of Case 3.

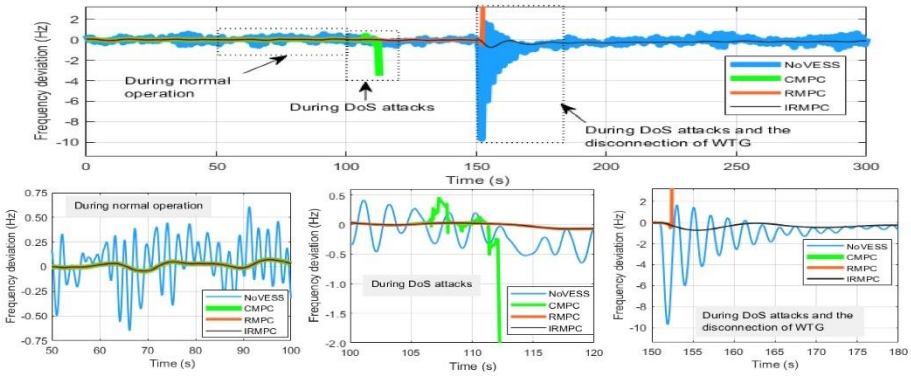


FIGURE 16. Frequency deviation of Case 3.

reduce the RoCoF to a value lower than that of the RMPC and NoVESS. However, NoVESS produced a higher RoCoF than RMPC.

The simulation results for Case 1 imply that, when using the VESS for virtual inertia control, the VESS controller should be designed under a DoS attack. If the VESS controller does not consider the effect of a DoS attack (i.e., CMPC), the control of the RoCoF and the frequency deviation will deteriorate.

Case 2: The simulation results for Case 2 are shown in Figs. 13 and 14 and can be explained by the following three situations.

2.1) During normal operation (50s-100s): The frequency and RoCoF deviations of the NoVESS were significantly higher than those of the CMPC, RMPC, and IRMPC, as in Case 1.

2.2) During DoS attacks (100s-130s): In this situation, the CMPC could not maintain the RoCoF within an allowance limit of approximately 119s. In contrast, RMPC and IRMPC can successfully maintain the RoCoF and frequency deviation within the allowance limit.

2.3) During DoS attacks and the disconnection of WTG (150s-180s): In this situation, IRMPC can reduce RoCoF to a value lower than that of RMPC and NoVESS. These results imply that IRMPC can improve microgrid virtual inertia control over RMPC and NoVESS.

In this case, it can be concluded that under a high-level DoS attack, IRMPC can reduce the RoCoF and frequency deviation better than NoVESS, CMPC, and RMPC.

Case 3: Figs. 15 and 16 show the simulation results for Case 3. The simulation results for Case 3 can be explained by the following three situations.

3.1) During normal operation (50s-100s): The frequency and RoCoF deviations of the NoVESS were significantly higher than those of the CMPC, RMPC, and IRMPC, as in Cases 1 and 2.

3.2) During DoS attacks (100s-120s): In this situation, the CMPC could not maintain the RoCoF within the maximum limit of approximately 112.5 s. In contrast, RMPC and IRMPC can successfully maintain the RoCoF and frequency deviation within the allowance limit.

3.3) During DoS attacks and the disconnection of WTG (150s-180s): In this situation, IRMPC can reduce RoCoF to a value lower than that of RMPC and NoVESS. However, RMPC could not maintain the RoCoF within an allowance limit of approximately 152s. These results imply that IRMPC can improve microgrid virtual inertia control over RMPC and NoVESS.

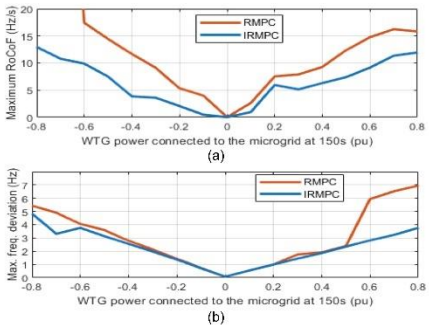


FIGURE 17. Simulation results when WTG connected/disconnected to the microgrid (a) maximum RoCoF (b) maximum frequency deviation.

In this case, it can be concluded that the proposed IRMPC is robust to variations in the system parameters.

In addition, to test the proposed IRMPC to the variation of the WTG connection/disconnection to the studied microgrid, the microgrid with the parameters of Case 1 was used. Figure 17 shows the simulation results of maximum RoCoF and maximum frequency deviation when WTG connection/disconnection to the microgrid from −0.8pu to 0.8 pu. The maximum RoCoF of IRMPC is lower than 20 Hz/s whereas that of RMPC is higher than 20 Hz/s when the disconnection of the WTG power is greater than 0.8 pu. The maximum frequency deviation of RMPC and IRMPC in Fig. 17 is high during the connection/disconnection of WTG, which is allowed during contingency (<±5 Hz) [36]. However, the frequency deviation of the proposed IRMPC is lower than that of the RMPC. These simulation results confirm that the proposed IRMPC exhibits superior performance over RMPC.

V. CONCLUSION

This paper proposes an improved resilient model predictive control (IRMPC) for virtual inertia emulation using a virtual energy storage system (VESS) under denial of service (DoS) attacks. The study results are summarized in detail below.

1) The IRMPC comprises an attack detector, an autoregressive (AR) signal estimator, and an MPC-based VESS controller. The AR parameters were optimized by a firefly algorithm with the objective of reducing the frequency and RoCoF deviations.

2) Under a DoS attack, the proposed IRMPC-based VESS can successfully provide virtual inertia emulation. Furthermore, the proposed IRMPC can reduce the rate of change of frequency (RoCoF) better than not using a VESS for virtual inertia control (No-VESS), conventional MPC-based VESS, and resilient MPC-based VESS.

3) When the microgrid inertia and damping properties are reduced, the proposed IRMPC can maintain the RoCoF and frequency deviation within acceptable ranges, whereas the No-VESS, conventional MPC-based VESS, and resilient MPC-based VESS cannot reduce the RoCoF and frequency deviation within acceptable ranges. These results indicate that the proposed IRMPC is robust to the microgrid parameter variations when subjected to DoS attacks.

REFERENCES

[1] S. K. Panda and B. Subudhi, "A review on robust and adaptive control schemes for microgrid," *J. Mod. Power Syst. Clean Energy*, vol. 11, no. 4, pp. 1027–1040, Jul. 2023.

[2] M. Farrokhabadi, C. A. Canizares, J. W. Simpson-Porco, E. Nasr, L. Fan, P. A. Mendoza-Araya, R. Tonkoski, U. Tamrakar, N. Hatziargyriou, D. Lagos, and R. W. Wies, "Microgrid stability definitions, analysis, and examples," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 13–29, Jan. 2020.

[3] P. S. Tadepalli and D. Pullaguram, "Distributed control microgrids: Cyber-attack models, impacts and remedial strategies," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 8, pp. 1008–1023, 2022.

[4] J. Fang, H. Li, Y. Tang, and F. Blaabjerg, "On the inertia of future more-electronics power systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 7, no. 4, pp. 2130–2146, Dec. 2019.

[5] T. Kerdphol, F. S. Rahman, M. Watanabe, and Y. Mitani, *Virtual Inertia Synthesis and Control* (Power Systems), 1st ed. Cham, Switzerland: Springer, 2021.

[6] U. Akram, N. Mithulananthan, M. Q. Raza, R. Shah, and F. Milano, "RoCoF restrictive planning framework and wind speed forecast informed operation strategy of energy storage system," *IEEE Trans. Power Syst.*, vol. 36, no. 1, pp. 224–234, Jan. 2021.

[7] J. Pahasa, P. Potejana, and I. Ngamroo, "MPC-based virtual energy storage system using PV and air conditioner to emulate virtual inertia and frequency regulation of the low-inertia microgrid," *IEEE Access*, vol. 10, pp. 133708–133719, 2022.

[8] M. Cheng, S. S. Sami, and J. Wu, "Benefits of using virtual energy storage system for power system frequency response," *Appl. Energy*, vol. 194, pp. 376–385, May 2017.

[9] H. Saberi, C. Zhang, and Z. Y. Dong, "Capacity of virtual energy storage system for frequency regulation services via a data-driven distributionally robust optimization method," *IEEE Trans. Power Syst.*, vol. 38, no. 3, pp. 2134–2147, May 2023.

[10] M. Shi, X. Chen, M. Shahidehpour, Q. Zhou, and J. Wen, "Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded AC microgrids," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 1953–1963, May 2021.

[11] M. Jamali, H. R. Baghaee, M. S. Sadabadi, G. B. Gharehpetian, and A. Anvari-Moghaddam, "Distributed cooperative event-triggered control of cyber-physical AC microgrids subject to denial-of-service attacks," *IEEE Trans. Smart Grid*, early access, Mar. 21, 2023, doi: 10.1109/TSG.2023.3259545.

[12] M. Chlela, D. Mascarella, G. Joós, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018.

[13] W. Yao, Y. Wang, Y. Xu, and C. Deng, "Cyber-resilient control of an islanded microgrid under latency attacks and random DoS attacks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5858–5869, Apr. 2023.

[14] S. Z. Tajalli, M. Mardaneh, E. Taherian-Fard, A. Izadian, A. Kavousi-Fard, M. Dabbaghjamanesh, and T. Niknam, "DoS-resilient distributed optimal scheduling in a fog supporting IIoT-based smart microgrid," *IEEE Trans. Ind. Appl.*, vol. 56, no. 3, pp. 2968–2977, May/Jun. 2020.

[15] S. Liu, P. Siano, and X. Wang, "Intrusion-detector-dependent frequency regulation for microgrids under denial-of-service attacks," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2593–2596, Jun. 2020.

[16] S. Hu, X. Ge, X. Chen, and D. Yue, "Resilient load frequency control of islanded AC microgrids under concurrent false data injection and denial-of-service attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 690–700, Jan. 2023.

[17] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for AC microgrids under cyber attacks," *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73–77, Jan. 2021.

[18] A. Bemporad, N. L. Ricker, and M. Morari, "Model predictive control toolbox user's guide," MATLAB R2023a, Math Works Inc., Natick, MA, USA, 2023.

[19] R. Ma, S. Basumallik, S. Eftekharnejad, and F. Kong, "A data-driven model predictive control for alleviating thermal overloads in the presence of possible false data," *IEEE Trans. Ind. Appl.*, vol. 57, no. 2, pp. 1872–1881, Mar./Apr. 2021.

[20] Q. Sun, K. Zhang, and Y. Shi, "Resilient model predictive control of cyber–physical systems under DoS attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4920–4927, Jul. 2020.

[21] G. Franzè, W. Lucia, and F. Tedesco, "Resilient model predictive control for constrained cyber-physical systems subject to severe attacks on the communication channels," *IEEE Trans. Autom. Control*, vol. 67, no. 4, pp. 1822–1836, Apr. 2022.

[22] A. Kusiak and Z. Zhang, "Short-horizon prediction of wind power: A data-driven approach," *IEEE Trans. Energy Convers.*, vol. 25, no. 4, pp. 1112–1122, Dec. 2010.

[23] Z. Ju, H. Zhang, and Y. Tan, "Deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified UFIR estimator," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3693–3705, May 2020.

[24] B. Zhang, C. Dou, D. Yue, J. H. Park, and Z. Zhang, "Attack-defense evolutionary game strategy for uploading channel in consensus-based secondary control of islanded microgrid considering DoS attack," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 2, pp. 821–834, Feb. 2022.

[25] J. Dowell and P. Pinson, "Very-short-term probabilistic wind power forecasts by sparse vector autoregression," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 763–770, Mar. 2016.

[26] N. U. Sheikh, H. J. Asghar, F. Farokhi, and M. A. Kaafar, "Do auto-regressive models protect privacy? Inferring fine-grained energy consumption from aggregated model parameters," *IEEE Trans. Services Comput.*, vol. 15, no. 6, pp. 3198–3209, Nov./Dec. 2022.

[27] H. E. Brown and C. L. Demarco, "Risk of cyber-physical attack via load with emulated inertia control," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5854–5866, Nov. 2018.

[28] X. S. Yang, *Engineering Optimisation: An Introduction With Metaheuristic Applications*. Hoboken, NJ, USA: Wiley, 2010.

[29] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Comput.*, vol. 10, no. 1, pp. 82–89, Jan./Feb. 2006.

[30] H. Zhu, X. You, and S. Liu, "Multiple ant colony optimization based on Pearson correlation coefficient," *IEEE Access*, vol. 7, pp. 61628–61638, 2019.

[31] J. Pahasa and I. Ngamroo, "PHEVs bidirectional charging/discharging and SoC control for microgrid frequency stabilization using multiple MPC," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 526–533, Mar. 2015.

[32] M. W. Altaf, M. T. Arif, S. Saha, S. N. Islam, M. E. Haque, and A. M. T. Oo, "Effective ROCOF-based islanding detection technique for different types of microgrid," *IEEE Trans. Ind. Appl.*, vol. 58, no. 2, pp. 1809–1821, Mar. 2022.

[33] C. Phurailatpam, Z. H. Rather, B. Bahrani, and S. Doolla, "Estimation of non-synchronous inertia in AC microgrids," *IEEE Trans. Sustain. Energy*, vol. 12, no. 4, pp. 1903–1914, Oct. 2021.

[34] D. Obradovic, M. Dijokas, G. S. Misyris, T. Weckesser, and T. Van Cutsem, "Frequency dynamics of the northern European AC/DC power system: A look-ahead study," *IEEE Trans. Power Syst.*, vol. 37, no. 6, pp. 4661–4672, Nov. 2022.

[35] T. Kerdphol, M. Watanabe, K. Hongesombut, and Y. Mitani, "Self-adaptive virtual inertia control-based fuzzy logic to improve frequency stability of microgrid with high renewable penetration," *IEEE Access*, vol. 7, pp. 76071–76083, 2019.

[36] *The Grid Code*, no. 6, Rev. 16, Nat. Grid Electr. Syst. Operator Ltd., London, U.K., Jan. 2023.

SATAWAT MUANGCHUEN received the B.Eng. and M.Eng. degrees in electrical engineering from the University of Phayao, Phayao, Thailand, in 2010 and 2015, respectively, where he is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, School of Engineering.

His research interest includes power system load frequency control.

JONGLAK PAHASA (Member, IEEE) received the B.Eng. degree in electrical engineering from the King Mongkut's Institute of Technology Ladkrabang (KMITL), Bangkok, Thailand, in 1997, the M.Eng. degree in electrical engineering from Chiang Mai University, Chiang Mai, Thailand, in 2007, and the D.Eng. degree in electrical engineering from KMITL, in 2011.

She is currently an Associate Professor with the School of Engineering, University of Phayao, Phayao, Thailand. Her current research interest includes the applications of artificial intelligence in power system stability and control.

ISSARACHAI NGAMROO (Senior Member, IEEE) received the B.Eng. degree in electrical engineering from the King Mongkut's Institute of Technology Ladkrabang (KMITL), Bangkok, Thailand, in 1992, and the M.Eng. and Ph.D. degrees in electrical engineering from Osaka University, Osaka, Japan, in 1997 and 2000, respectively.

He is currently a Professor with the Department of Electrical Engineering, School of Engineering, KMITL. He is also the Leader of the Senior Research Scholar Project of "Intelligent control-based smart renewables for power system stability enhancement" granted by the National Research Council of Thailand. His research interests include power system stability, dynamic, and control.

APPENDIX C Proceedings Enhanced Resilient Model Predictive Control Electrolyzers for Frequency Regulations Under Severe Denial – of – Service Attacks

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 11 April 2024, accepted 2 May 2024, date of publication 8 May 2024, date of current version 15 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3397874

RESEARCH ARTICLE

Enhanced Resilient Model Predictive Control Electrolyzers for Frequency Regulations Under Severe Denial-of-Service Attacks

SATAWAT MUANGCHUEN, JONGLAK PAHASA, (Member, IEEE), AND CHAWASAK RAKPENTHAI, (Member, IEEE)
Department of Electrical Engineering, School of Engineering, University of Phayao, Phayao 56000, Thailand
Corresponding author: Jonglak Pahasa (jonglak.pa@up.ac.th)

This work was supported by the University of Phayao, Thailand.

ABSTRACT Proton exchange membrane electrolyzers (PEMEL) installed with renewable energy resources can be used for power system ancillary services such as frequency regulation and virtual inertia emulation. However, the performance of PEMEL-based frequency ancillary services is threatened by cyberattacks that compromise the communication control. Considering denial-of-service (DoS) attacks on PEMEL communication, this paper proposes an enhanced resilient model predictive control (ER-MPC) for a PEMEL controller. The proposed ER-MPC consists of two procedures. First, the combination of autoregressive (AR) model-based prediction method and hold signal method is used to reconstruct attacked signals during severe DoS attacks. Then a model predictive control (MPC) is used to compute the control signal for PEMEL stack. The objective of ER-MPC-based controlling of PEMEL is to regulate the frequency deviation during contingency and normal operation under severe DoS attack. The effectiveness of the proposed ER-MPC was compared with that of AR-based resilient MPC and resilient MPC methods. The simulation results revealed that the proposed ER-MPC successfully improved microgrid frequency regulations under severe DoS attacks. In addition, the proposed ER-MPC-based PEMEL has a performance effect over other techniques in terms of the reduction in frequency deviation and the rate of change of frequency during severe DoS attacks, disconnection, and successful connection of wind turbine generation.

INDEX TERMS Microgrid, frequency regulation, resilient MPC, denial-of-service attack, proton exchange membrane electrolyzers.

I. INTRODUCTION

Renewable energy sources (RES) based on distributed generation (DG), such photovoltaic and wind turbines, are typically connected to power systems via power electronic converters. The connection of DG-based RES to the power system via power electronic converters causes a reduction in the overall system stability, reduces the power system inertia, and increases the frequency fluctuation [1], [2], [3]. Conventionally, battery energy storage systems (BESS) have been used to improve the frequency regulation and virtual inertia. Nonetheless, the BESS's investment and maintenance costs are high, and it cannot be destroyed at the end of its lifetime [4], [5]. Therefore, it is necessary to use other devices for frequency regulation.

Green hydrogen electrolyzers, that is, hydrogen derived from RES, are a promising choice for frequency regulation and virtual inertia improvement [6]. Green hydrogen has attracted considerable attention and shows great promise because it connects renewable electricity to various end-use applications which direct electrification is impractical [6]. Hossain et al. [7] proposed proton exchange membrane

The associate editor coordinating the review of this manuscript and approving it for publication was Mouloud Denai.

electrolyzers (PEMEL) for power system frequency control. In [8], it was suggested to model a PEMEL's dynamic electrical circuit for frequency stability, resilience, and sensitivity studies in a power grid. In [9], the dynamic modeling of a pressurized alkaline water electrolyzer has been proposed. The application of hydrogen electrolysis devices in virtual inertia and frequency regulation was studied by Dozein et al. [6]. The findings demonstrate that PEMEL units are viable options for future power systems' virtual inertia regulation, and frequency control auxiliary services. However, the controller used for virtual inertia and frequency regulation in [6] consists of a deviation detector and integrator, which are insufficient for the high penetration of intermittent RES. Therefore, it is necessary to improve the controller design for the PEMEL-based frequency ancillary services. In addition, Dozein et al. [6] did not study the effect of cyber-attacks on the PEMEL controllers. For cyber-physical systems, the effect of cyber-attacks should be studied in detail, especially in the case of ancillary services from multiservice equipment in the power system such as PEMEL.

Power grids are susceptible to various cyber-attacks such as false data injection and denial-of-service (DoS) attacks. False data injection attacks can damage the data integrity of the grid, whereas denial-of-service attacks can jeopardize communication network resources and services that are accessible to the power grid [10]. Several techniques such as fallback control [10], robust even-triggered control [11], [12], and resilience control [13], [14] have been proposed to reduce the impact of denial-of-service attacks on power system frequency regulation. Among these techniques, resilient control is an effective method for solving cyber-physical system issues. Resilient control aims to maintain an acceptable level of operational regularity in the presence of DoS attacks, while maintaining system robustness against disturbances [15]. The resilient load frequency regulation of islanded microgrids under simultaneous DoS and false data injection attacks has been proposed in [13]. In [14], resilient load frequency regulation of multi-area power systems under DoS attack was examined. However, the controllers in [13] and [14] were designed based on the estimation of a microgrid state-space model. When a signal that provides state-space is compromised by cyberattacks, state-space estimation during denial-of-service attacks may suffer.

Furthermore, model predictive control (MPC), a widely accepted adaptive control algorithm, is utilized in numerous practical applications [4], [5]. MPC employs a plant's dynamic model to project the optimal control signal while optimizing the plant's output. Resilient model predictive control represents an enhanced form of MPC, specifically designed to manage cyber-physical systems in the presence of denial-of-service (DoS) attacks [15]. A data driven resilient MPC for linear time invariant (LTI) systems against DoS attacks was proposed in [16]. Additionally, a robust and resilient distributed MPC for cyber-phisical systems of four ground vehicles control problems against DoS attacks was proposed in [17]. However, the attacked signal of the robust and resilient distributed MPC in [17] and the resilient MPC in [15] uses a previous signal before the DoS attacks instead of an attacked signal. The holding signals based methods as provided in [15] and [17] was improved by using an autoregressive model-based prediction, as proposed in [5].

In order to address this issue, load frequency control using resilient model predictive control (RMPC) was introduced in [15]. During cyberattacks, the RMPC maintained a control signal that was comparable to that which it had before. However, holding signal for long time may degrade the control performance. Thus, to improve the resilient control method, an improved resilient model predictive control was proposed in [5] to mitigate the effectiveness of denial-of-service attacks in microgrid virtual inertia and frequency regulation. Autoregressive (AR) model-based prediction has been used to predict feedback-attacked signals before model predictive control (MPC) computations. The study results imply that improved resilient model predictive control can effectively improve virtual inertia emulation. Nonetheless, the improved resilient model predictive control in [5] may deteriorate when the system encounters severe denial of service attacks because it may not accurately predict data when the unknown sample is far from the known samples, particularly in the case of a severe DoS attack.

Based on the above premises, considering severe denial of service attacks, this study intends to investigate the combination of hold signal-based resilient control [15] and autoregressive-based resilient MPC to improve the PEMEL controller and provide microgrid frequency regulations under severe denial-of-service attacks. The primary contributions of this study are as follows.

(1) We propose an enhanced resilient model predictive control (ER-MPC) for controlling PEMEL to improve frequency regulations under severe denial-of-service attacks that have not been studied in the literature.

(2) We propose a new control technique that extends autoregressive model-based prediction by feeding MPCs (improved resilient MPC [5]) by considering severe denial-of-service attacks. The error in autoregressive-based predictions may be high when denial-of-service attacks occur over long periods. Therefore, the holding signal, as in [15], is applied to avoid prediction errors.

(3) The proposed enhanced resilient MPC for the PEMEL control method can be successfully used with severe DoS attackers.

The remainder of this paper is organized as follows. The formulation of this problem is discussed in Section II. Section III provides details of the proposed enhanced resilient model predictive control under severe denial-of-service attacks. Section IV presents the simulation findings and related remarks. Section V concludes the paper.

II. STUDY SYSTEM AND PROBLEM FORMULATION

This section introduces the study system and formulation of the problem. First, a microgrid frequency regulation model under cyber-attacks is introduced. Next, we explain

the PEMEL model for frequency regulation. Subsequently, control of a large-scale PEMEL stack was proposed. Finally, the denial-of-service attack model is explained.

A. MICROGRID MODEL FOR FREQUENCY CONTROL UNDER DOS ATTACKS

Figure 1 depicts the microgrid with the suggested enhanced resilient MPC-based PEMEL for frequency regulation during denial-of-service attacks. In the transmission channel between the "Microgrid" and "PEMEL controller" blocks, denial-of-service attacks were employed to disrupt communication services, which harms system functionality [5]. Controller performance may suffer during denial-of-service attacks. As a result, the ER-MPC, the PEMEL controller, ought to be built to lessen the impact of a denial-of-service attack on control actions. In order to improve microgrid frequency regulation during denial-of-service attacks, this work suggests an improved resilient model predictive control for proton exchange membrane electrolyzers.

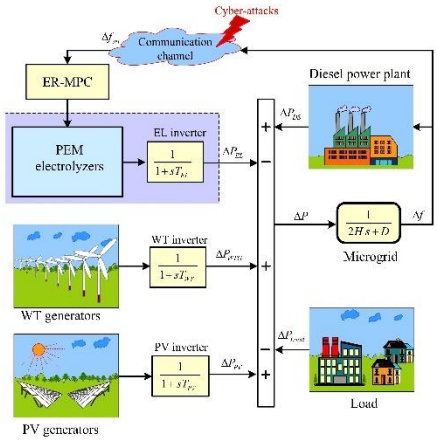


FIGURE 1. Microgrid with the proposed ER-MPC-based PEMEL for virtual inertia and frequency regulations under DoS attacks.

As shown in Fig. 1, the microgrid frequency deviation can be expressed as

$$\Delta f = \frac{1}{2H\,s + D}\Delta P \tag{1}$$

$$\Delta P = \Delta P_{DS} + \Delta P_{PV} + \Delta P_{WTG} - \Delta P_{Load} - \Delta P_{EL} \tag{2}$$

where H stands for the microgrids' inertia, D for its damping qualities, P_{DS} for the diesel generators' power, P_{PV} for the photovoltaic generators, power, P_{WTG} for the wind turbine generators' power, P_{Load} for the load demand's power, P_{EL} for the PEMEL's power, and Δ is the deviation of the signal.

The nominal system frequency varies as a result of the discrepancy between the generated power and the load demand. If the generated power is less than the load, the generator units' speed and frequency begin to decrease ($-\Delta P$). The generators' frequency and speed start to rise when the generated power surpasses the load ($+\Delta P$).

The frequency deviation caused by the intermittent nature of renewable energies such as photovoltaic generator and wind power generation in Fig. 1 can be reduced by controlling the PEMEL. However, owing to the distribution control of microgrids through communication channels, cyberattacks may deteriorate the control performance of PEMEL to suppress frequency fluctuations. Thus, an enhanced resilient model predictive control has been used to control PEMEL.

Additionally, Fig. 2 shows the diesel power plant model used in this study. The diesel power plant was thought to be situated near to the control center. Consequently, the effect of DoS attacks on diesel power plant control is not taken into account in this study.

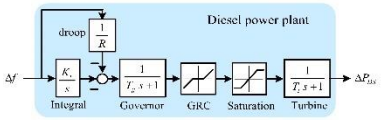


FIGURE 2. Diesel power plant model used in the study.

B. PEMEL MODEL FOR FREQUENCY REGULATIONS

Hydrogen electrolysis is a power-to-gas storage technology that makes it easier to integrate intermittent renewable energy sources on a wide scale into future energy systems. Figure 3 shows the dynamic properties of a PEMEL stack, which is based on the dynamic electrical equivalent model for frequency regulation [8].

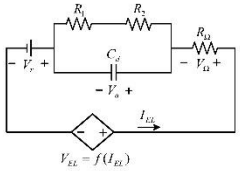


FIGURE 3. PEMEL dynamical electrical equivalent circuit [8].

The following first-order differential equations can be used to express the dynamic properties of the circuit in Fig. 3.

$$\frac{dV_a}{dt} = \frac{I_{EL}}{C_d} - \frac{V_a}{T_{EL}} \tag{3}$$

where V_a is the activation voltage drop, I_{EL} is the PEMEL current, C_d is the capacitor, and T_{EL} is the first-order time constant of PEMEL. The cathodic/anodic electrode separating two different types of materials causes T_{EL} due to charge accumulation/decumulation brought on by electrons moving from one electrode to another. T_{EL} also known as the charge double-layer effect and can be expresses as

follows [7], [8].

$$T_{EL} = (R_1 + R_2)\, C_d = R_d\, C_d \tag{4}$$

where R_1 and R_2 are the PEMEL resistances showing the activation losses, and R_d is the equivalent resistance. C_d shows how a change in the electrolyzer's current can dynamically affect the PEMEL, or charge layer, at the electrode-electrolyte interface.

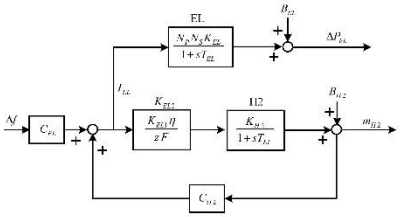


FIGURE 4. PEMEL model for frequency regulations used in this study.

The linearized model of the PEMEL for power system frequency regulation modified from [7] and [8] is shown in Fig. 4. T_{EL} needs to be taken into account when using PEMEL to regulate power system frequency. The regulation and adjustment of PEMEL power consumption are delayed by T_{EL} in the event of rapid changes in the system frequency. Therefore, the power consumption of PEMEL can be described by the Laplace transform as follows [7], [8].

$$P_{EL}(s) = \frac{K_{EL}}{1 + sT_{EL}} I_{EL}(s) + B_{EL} \tag{5}$$

where K_{EL} and B_{EL} are the coefficients and initial PEMEL power consumption, respectively.

The downstream hydrogen production rate m_{H2} [Nm^3/s], can be expressed as:

$$m_{H2}(s) = K_{EL1} \frac{\eta_F\, I_{EL}(s)}{z\, F} \tag{6}$$

where K_{EL1} is the coefficient converts mole/s to Nm^3/s, z is the electron density, F is Faraday's constant, and η_F stands for Faraday efficiency.

The time delay T_{EL} may change the hydrogen production submodel since the rate of hydrogen synthesis is a linear function of current. Thus, the hydrogen production sub-model can be expressed as

$$m_{H2}(s) = \frac{K_{EL2} K_{H2}}{1 + sT_{EL}} I_{EL}(s) + B_{H2} \tag{7}$$

$$K_{EL2} = K_{EL1}\left(\frac{\eta_F}{zF}\right) \tag{8}$$

where K_{H2} is the hydrogen coefficients and B_{H2} is the initial hydrogen production rate.

C. CONTROL OF A PEMEL STACK

In order to produce the necessary output voltages, currents, and power for grid applications, a PEMEL stack is built using series-parallel connections. This can be represented as

$$V_{EL,\,stack} = N_S\, V_{EL} \tag{9}$$

$$I_{EL,\,stack} = N_P\, I_{cell} \tag{10}$$

$$P_{EL,\,stack} = V_{EL,\,stack}\, I_{EL,\,stack} \tag{11}$$

where N_S and N_P are the number of series- and parallel-connected cells per stack, respectively.

The PEMEL stack current ($I_{EL,\,stack}$) can be adjusted to control the downstream hydrogen generation rate and power consumption, as shown in equations (10) and (11). The aim of hydrogen production control is to maintain a regulated downstream rate of hydrogen generation. The difference between the current rate of hydrogen production, indicated by m_{pre}, and the previous value, indicated by m_{past}, is therefore used to change the downstream hydrogen generation rate of the PEMEL stack. This difference can be stated as

$$\Delta m_{H2}(s) = m_{pre}(s) - m_{past}(s) \tag{12}$$

Thus, the PEMEL current deviation can be written as,

$$\Delta I_{EL}(s) = C_{H2}(s) \cdot \Delta m_{H2}(s) \tag{13}$$

where C_{H2} is a built-in controller that controls hydrogen production rate.

To provide the frequency regulation capacity, an additional controller, C_{EL}, is included to regulate the hydrogen generation rate for frequency regulation [8]. Thus, (13) can be revised as follows.

$$\Delta I_{EL}(s) = C_{H2}(s) \cdot \Delta m_{H2}(s) + C_{EL}(s) \cdot \Delta f(s) \tag{14}$$

where Δf stands for the power systems frequency deviations.

The PEMEL power adjustment is calculated as follows by replacing (14) in equation (11).

$$\left.\begin{aligned} \Delta P_{EL}(s) = {} & \tfrac{K_{EL}}{1+sT_{EL}} C_{H2}(s) \cdot \Delta m_{H2}(s) \\ & + \tfrac{K_{EL}}{1+sT_{EL}} C_{EL}(s) \cdot \Delta f(s) \end{aligned}\right\} \tag{15}$$

According to (15), there are two parameters that are related to the PEMEL operational power adjustment: (1) the fluctuation in the rate of hydrogen generation (Δm_{H2}), and (2) the variation in frequency (Δf). The rate of hydrogen production variation can be ignored due to the short duration of the frequency adjustment method (maximum 30 s) [8]. As a result, it is possible to regard the rate of hydrogen creation as constant during this time [8]. Consequently, (15) can be expressed simply as:

$$\Delta P_{EL}(s) = C_{EL}(s) \cdot \frac{K_{EL}}{1 + sT_{EL}} \cdot \Delta f(s) \tag{16}$$

In this study, the ER-MPC is used to control the PEMEL for frequency regulation. Δf is the ER-MPC input which is used to compute control signal for PEMEL controller. Thus, when

using ER-MPC to control PEMEL for frequency regulation, (16) can be expressed as.

$$\Delta P_{EL}(s) = u_{ER-MPC}(s) \cdot \frac{K_{EL}}{1 + sT_{EL}} \tag{17}$$

In this work we assumed that the ER-MPC controller is located near PEMEL stack. Thus, the DoS attack caused Δf deteriorates and must be improved by the proposed ER-MPC as explained in Section III.

D. MODELING OF DENIAL-OF-SERVICE ATTACK

Denial-of-service attacks transmit erroneous and useless data to system components in order to occupy or use restricted resources [5], [13]. The timing of the denial-of-service attack occurrence is shown by:

$$\Im(0, \infty) \triangleq \bigcup_{l \in \mathbb{N}} [T_{on,l},\ T_{off,l}] \tag{18}$$

where T stands for sample duration, $T_{on,l} \in [T_{on}^{\min}, T]$, $l \in \mathbb{N}$ stands for the time when a denial-of-service attack first occurs, and $T_{off,l} \in [T_{off}^{\min}, T]$, $l \in \mathbb{N}$ stands for the time when the denial-of-service attack ends. The duration of the denial-of-service attack was $T_{off} - T_{on}$ and each denial-of-service attack had a trigger time of $T_{on} < T_{off} \leq T$.

The following represents the model of a nonperiodic random variable denial-of-service attack at all activation times:

$$S_{DoS}(t) = \begin{cases} 0, & t \in \Im(0, \infty) \\ 1, & t \notin \Im(0, \infty) \end{cases} \tag{19}$$

where $S = 1$ indicates normal transmission and $S = 0$ indicates the occurrence of denial-of-service attacks.

III. PROPOSED ER-MPC FOR PEMEL CONTROL UNDER SEVERE DOS ATTACKS

This section describes the enhanced resilient model predictive control-based PEMEL controller that is suggested for use in the event of major denial-of-service attacks on microgrid frequency auxiliary services. Firstly, we describe how to estimate the frequency deviation, or feedback signal, in the event of a denial-of-service attack. After that, a description of the enhanced resilient model predictive control for PEMEL frequency regulation control is provided.

A. METHODS FOR ESTIMATING FEEDBACK SIGNAL DURING DOS ATTACKS

Figure 5 shows the methods used in this study for estimating signals during DoS attacks. More details are provided below.

(1) Hold signal technique: Fig. 5(a) shows the hold signal method [13] when system encounters cyberattack. The holding signal method is defined as,

$$\Delta \tilde{f}(t) = \Delta f(t-1) \tag{20}$$

where $\Delta \tilde{f}(t)$ is the frequency deviation reconstructed by the holding method, and $\Delta f(t-1)$ is the actual frequency deviation at time $t-1$, which is transmitted through the communication link before the DoS attack occurs.

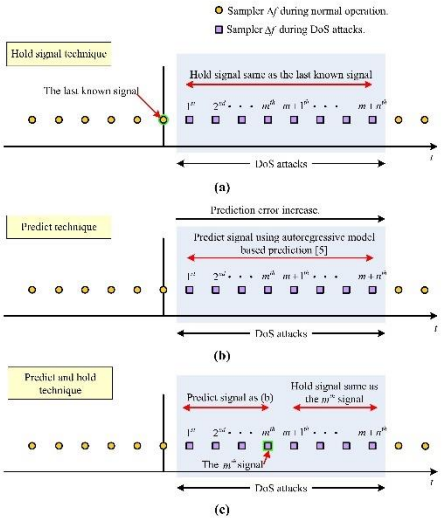


FIGURE 5. Methods for estimating signal during DoS attacks (a) hold signal technique (b) prediction technique (c) predict and hold technique.

The holding signal may deteriorate when the attacked signals are significantly different from the last known signal (i.e., when the hold signal is the same as the last known signal).

(2) Predict technique: In this study, the autoregressive (AR) model was used to predict frequency deviation (Δf) during a DoS attack.

Conventional statistical methods, such as AR models, can be applied to time-series data prediction [5]. An AR stochastic process's current output depends linearly on its previous outputs. The AR model for the prediction frequency deviation is defined as [5],

$$\Delta \tilde{f}(t) = \sum_{k=1}^{p} b_k \Delta f_{com}(t-k) \tag{21}$$

where $\Delta \tilde{f}$ is the predicted frequency deviation, t indicates the current time instant, p is the order of the AR model, and b_k is the weight of the AR model. Δf_{com} is the frequency deviation sent via a communication link that has been harmed by denial-of-service attacks.

Figure 5(b) shows the prediction method using autoregressive model-based prediction [5], as provided in (24). Error in the prediction method may increase when the prediction samples are far from the last known signal. Therefore, the prediction method may deteriorate when used to predict an attack signal during a severe DoS attack.

(3) Predict and hold technique: To improve the performance of the reconstruction signal for a resilient MCP, the prediction-and-hold technique, as shown in Fig. 5(c), is proposed herein. The combination of the prediction method and hold signal method improves the performance of the control techniques owing to the long time of unknown data during the DoS attack.

B. PROPOSED ENHANCED RESILIENT MPC-BASED PEMEL CONTROL FOR FREQUENCY REGULATIONS

As shown in Fig. 1, the PEMEL controller receives a frequency variation through a communication link that is vulnerable to denial-of-service (DoS) attacks. The frequency deviations become worse during a denial-of-service attack, and the traditional MPC-based PEMEL's capacity to control frequency decreases. Thus, as shown in Fig. 6, our study suggests an enhanced resilient MPC-based PEMEL for frequency regulation. Additionally, before the frequency deviation signal is sent to the MPCs, it is preprocessed with the block "Enhanced attack detector and signal estimator" as shown in Fig. 7, added.

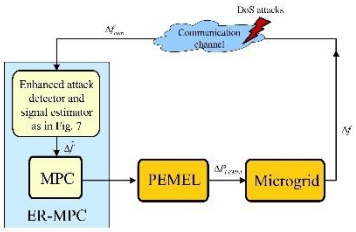


FIGURE 6. The proposed ER- MPC-based PEMEL control under denial-of-service attack.

IV. SIMULATION RESULTS AND DISCUSSION

This section presents the results of the simulation along with a discussion. Firstly, the investigation of the impact of denial-of-service attacks on microgrid frequency regulation using several techniques for feedback signal estimation is presented. The simulation settings are then described. The simulation results are then shown, followed by a discussion.

A. STUDY DOS-ATTACK EFFECTED TO MICROGRID FREQUENCY ROGULATION WHEN USING DIFFERENT METHODS FOR ESTIMATING FEEDBACK SIGNAL

The autoregressive model uses historical data to forecast future events. The autoregressive model can therefore be improved to forecast frequency deviation during denial-of-service attacks by examining the signals' relationship with denial-of-service attack levels.

The efficiency of the proposed enhanced resilient model predictive control (ER-MPC) was compared with that of resilient MPC (R-MPC) and autoregressive-based resilient MPC (ARR-MPC). R-MPC was designed based on the hold signal, as shown in [15] and Fig. 5 (a). The results for

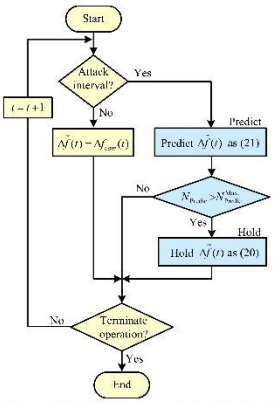


FIGURE 7. An enhanced attack detector and signal estimator.

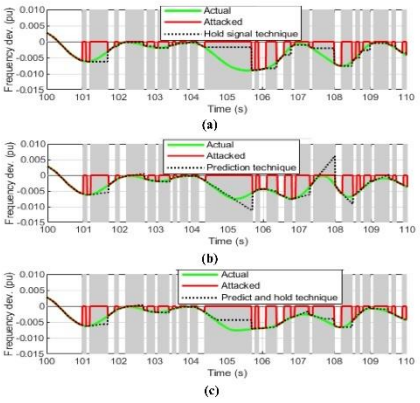


FIGURE 8. Frequency deviation when DoS probability of zero = 0.6 (a) hold signal (b) prediction (c) predict and hold techniques.

microgrids operated with R-MPC under normal and severe DoS attacks are shown in Figs. 8 (a) and 9 (a), respectively. The ARR-MPC was designed based on the hold signal, as shown in [5] and Fig. 5 (a). The results for the microgrid operated with the ARR-MPC under normal and severe DoS attacks are shown in Figs. 8 (b) and 9 (b), respectively. The proposed ER-MPC was designed based on a combination of the prediction and hold signals, as shown in Fig. 5 (c). The results for the microgrid operated with the ER-MPC under normal and severe DoS attacks are shown in Figs. 8 (c) and 9 (c), respectively.

Note: In a realistic scenario, the DoS attack probability of zero is 0.6 and 0.85, as shown in Figs. 7 and 8, respectively, may not occur. However, learning-based attacks proposed in [18] show that an attacker's success rate is near 0.9, which is close to the cyber-attack rate used in

this study. Additionally, current researchers have focused on solving the problems of severe DoS attacks, such as deterministic network calculus-based H∞ load frequency control of multiarea power systems [20], and data-driven resilient MPC to the stabilization problem of unknown linear time invariant (LTI) systems [16]. Therefore, severe DoS attacks, as shown in Figs. 7 and 8, can be used to test the performance of the load-frequency control problem to confirm the performance of the proposed method.

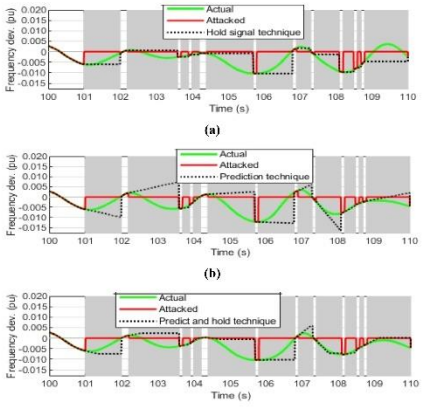


FIGURE 9. Frequency deviation when DoS probability of zero = 0.85 (a) hold signal (b) prediction (c) predict and hold techniques.

B. SIMULATION SETTING

MATLAB/Simulink and the MPC toolbox [18] was used to evaluate the effectiveness of the enhanced resilient MPC (ER-MPC) for PEMEL in controlling microgrid frequency deviation under denial-of-service attacks. The study system was the microgrid, which is depicted in Fig. 2. Table 1 displays the microgrid data [4], [5], and the PEMEL parameters [7], [8].

Figure 10 shows load demand and WTG power of the case studies. The load demands of Case 1 were higher than those of Case 2 for the first simulation at 75-130 s. Then, after 150 s, the load demand in Case 2 was higher than that in Case 1 until 240 s. For case 1, it is assumed that at 120 s, WTG disconnects 0.1 pu and reconnects 0.12 pu at 180 s, respectively. The microgrid's stability is decreased when the WTG is disconnected. As a result, the frequency deviation exceeds the nominal values and could go up to the maximum frequency permitted.

C. SIMULATION RESULTS AND DISCUSSION

Figures 11 (a) – (d) show the frequency deviations of Case 1 when the DoS probabilities of zero were 0.65, 0.75, and 0.85, respectively. When the DoS probability of zero was 0.55, as shown in Fig. 11 (a), the frequency deviations of the

TABLE 1. Microgrid and PEMEL parameters values.

Parameters	Values	Parameters	Values
f_{ref}	50 Hz	P_{EL}	5 MW
H	0.06 s	K_{EL}	1.6 W/A
D	0.12 pu	K_{EL1}	4841.4
T_g	0.1 s	T_{EL}	37 s
T_t	0.4 s	C_{dl}	37 F
R	2.4 (Hz/pu.MW)	B_{H2}	0.5 m^3/s
K_1	0.2 s	B_{PEL}	82 W
		K_{H2}	0.028 m^3/As

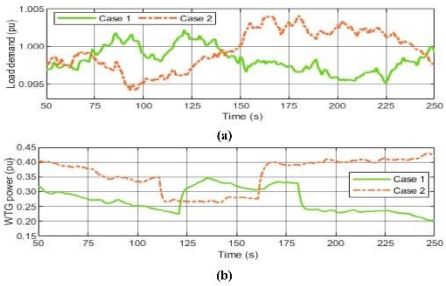


FIGURE 10. Load demand and WTG power of the case studies (a) load demand (b) WTG power.

R-MPC, ARR-MPC, and proposed ER-MPC did not seem to differ. When the DoS probability zero was 0.65, as shown in Fig. 11 (b), the frequency deviations of the R-MPC and ARR-MPC were slightly higher than those of the ER-MPC. When the DoS probability of zero was 0.75, as shown in Fig. 11 (c), the frequency deviations of the R-MPC were higher than those of the ARR-MPC and ER-MPC. When the DoS probability of zero was 0.85, as shown in Fig. 11 (d), the frequency deviations of the R-MPC and ARR-MPC were clearly higher than those of the ER-MPC. The maximum frequency deviation increased when the DoS probability of zero increased.

Figure 12 displays the simulation results for Case 1 when the DoS probability is zero = 0.85. Figure 12 (a) shows the rate of change in the frequency of the proposed and the comparison methods. The proposed ER-MPC can maintain the RoCoF of the microgrid within acceptable ranges. The R-MPC maintains the RoCoF, while the ARR-MPC deteriorates. Figure 12 (b) shows the hydrogen production rate of the PEMEL stack. Figure 12 (c) shows the power of the PEMEL stack. The hydrogen production rate was consistent with that of the PEMEL power.

Figures 13 (a) – (d) show the frequency deviations of Case 1 when the DoS probabilities of zero were 0.65, 0.75, and 0.85, respectively. When the DoS probability of zero

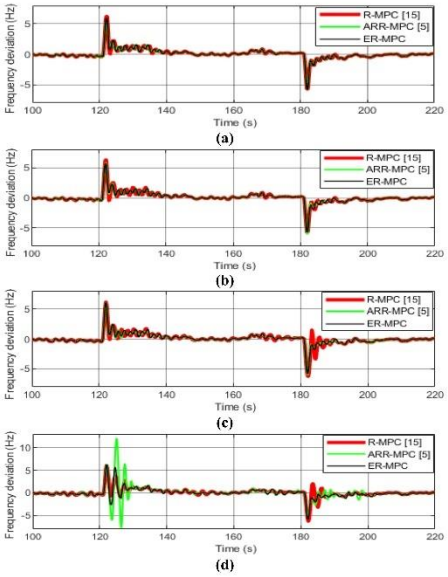


FIGURE 11. Frequency deviation of case 1, (a) DoS probability of zero = 0.55 (b) DoS probability of zero = 0.65 (c) DoS probability of zero = 0.75 (d) DoS probability of zero = 0.85.

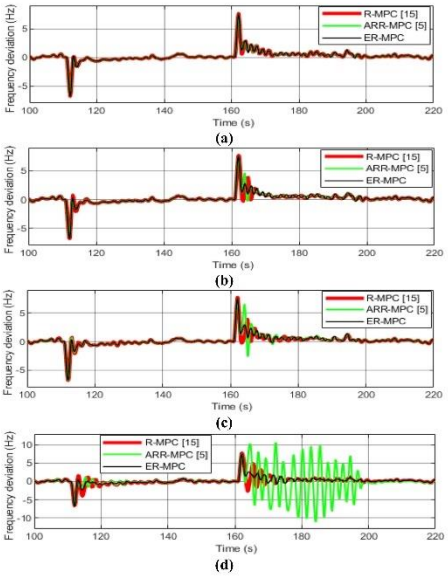


FIGURE 13. Frequency deviation of case 2. (a) DoS probability of zero = 0.55 (b) DoS probability of zero = 0.65 (c) DoS probability of zero = 0.75 (d) DoS probability of zero = 0.85.

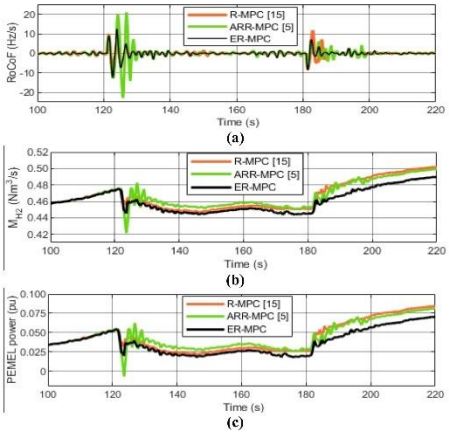


FIGURE 12. Simulations results of Case 1 when DoS probability of zero = 0.85 (a) RoCoF (b) hydrogen production rate (c) power of PEMEL stack.

was 0.55, as shown in Fig. 13 (a), the frequency deviations of the R-MPC, ARR-MPC, and proposed ER-MPC did not seem to differ. When the DoS probability of zero was 0.65, as shown in Fig. 13 (b), the frequency deviations of R-MPC and ARR-MPC were slightly higher than those of ER-MPC. When the DoS probability of zero was 0.75, as shown in Fig. 13 (c), the frequency deviations of the R-MPC were higher than those of the ARR-MPC and ER-MPC. When the DoS probability of zero is 0.85, as shown in Fig. 13 (d), the frequency deviations of the R-MPC and ARR-MPC are clearly higher than those of the ER-MPC. The maximum frequency deviation increased when the DoS probability of zero increased.

Figure 14 displays the simulation results for Case 2 when the DoS probability of zero 0.85. Figure 14 (a) shows the rate of change in the frequency of the proposed and the comparison methods. The proposed ER-MPC can maintain the RoCoF of the microgrid within acceptable ranges. The R-MPC maintains the RoCoF, while the ARR-MPC deteriorates. Figure 14 (b) shows the hydrogen production rate of the PEMEL stack. Figure 14 (c) shows the power of the PEMEL stack. The hydrogen production rate was consistent with that of the PEMEL power. These results confirmed that the proposed ER-MPC can improve the performance of the control method under severe DoS attacks.

Additionally, to test the performance of the proposed ER-MPC for a DoS probability of zero, a microgrid with the parameters of Cases 1 and 2 was used. Ten random DoS patterns are generated. Each random DoS pattern changed the probability of zero from 0.00 to 0.85. The DoS probability

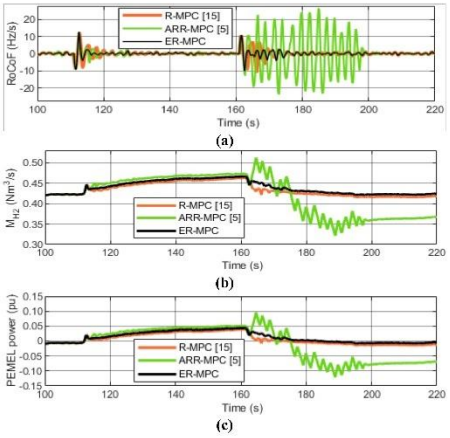


FIGURE 14. Simulations results of Case 2 when DoS probability of zero = 0.85 (a) RoCoF (b) hydrogen production rate (c) power of PEMEL stack.

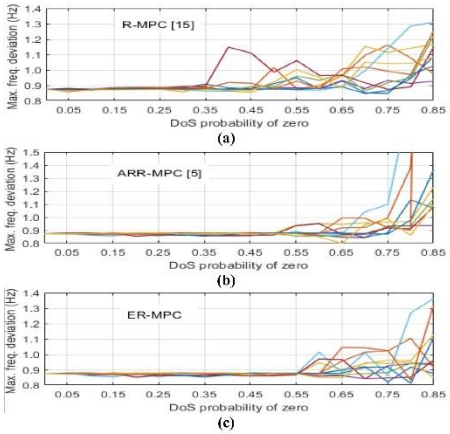


FIGURE 16. Simulation results of Case 2 when DoS probability of zero is varied from 0.00 to 0.85 (a) R-MPC (b) ARR-MPC (c) ER-MPC.

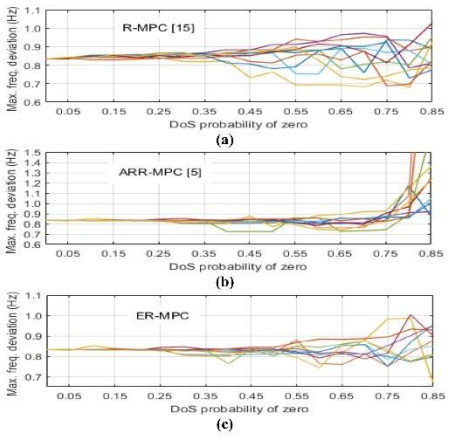


FIGURE 15. Simulation results of Case 1 when DoS probability of zero is varied from 0.00 to 0.85 (a) R-MPC (b) ARR-MPC (c) ER-MPC.

of zero is "0.00" means there are no DoS occures in the transmission line between the microgrid control center and the PEMEL controller. Note that in this case, the ability of the proposed control method to regulate frequency was tested. Thus, the WTG was not connect/disconnect to the microgrid.

Figure 15 shows the simulation results of Case 1 when the DoS probability of zero was varied from 0.00 to 0.85. The simulation results in Fig. 15 demanstrate that when the DoS probability of zero lower than 0.25, the maximum frequency deviation of the R-MPC, ARR-MPC and the proposed ER-MPC methods were not different and close to the maximum frequency deviation in the case of DoS probability of zero was "0.00". When the DoS probability of zero was higher than 0.25, the maximum frequency deviation of the three methods was high, especially when the DoS probability of zero was 0.85. However, the maximum frequency deviation of the proposed ER-MPC is lower than those of the R-MPC and ARR-MPC.

Figure 16 shows the simulation results of Case 2 when the DoS probability of zero was varied from 0.00 to 0.85. When the DoS probability of zero lower than 0.35, 0.47, and 0.55, respectively, the maximum frequency deviation of the three method were not different and close to the maximum frequency deviation in the case of DoS probability of zero was "0.00". When the DoS probability of zero was higher than 0.35, 0.47, and 0.55, the maximum frequency deviation of the three methods was high, especially in the case where the DoS probability of zero was 0.85. However, the maximum frequency deviation of the proposed ER-MPC is lower than that of the R-MPC and ARR-MPC.

The simulation results in Figs. 15 and 16 confirm that the proposed ER-MPC exhibits superior performance over R-MPC and IRR-MPC when using the PEMEL for the frequency regulation of the microgrid.

V. CONCLUSION

This research presents an enhanced resilient model predictive control (ER-MPC) for microgrid frequency regulation against severe denial-of-service attacks using proton exchange membrane electrolyzers (PEMEL). The proposed ER-MPC combines autoregressive model-based prediction and holds signals for resilient model predictive control to enhance the control effect when subject to severe DoS attacks. The efficacy of the suggested ER-MPC was compared with that of the autoregressive-based robust model predictive

control (ARR-MPC) and resilient model predictive control (R-MPC) techniques. Based on the simulation findings, it was found that the proposed ER-MPC can effectively enhance microgrid frequency controls compared to the R-MPC and ARR-MPC by lowering frequency deviation and rate of change of frequency during severe denial-of-service attacks. Additionally, the study results show that the combination of prediction and hold signals for resilient model predictive control is appropriate for PEMEL control of frequency regulation under severe denial-of-service attacks.

REFERENCES

[1] T. Kerdphol, F. S. Rahman, M. Watanabe, and Y. Mitani, *Virtual Inertia Synthesis and Control* (Power Systems), 1st ed. Cham, Switzerland: Springer, 2021.

[2] J. Fang, H. Li, Y. Tang, and F. Blaabjerg, "On the inertia of future more-electronics power systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 7, no. 4, pp. 2130–2146, Dec. 2019.

[3] S. K. Panda and B. Subudhi, "A review on robust and adaptive control schemes for microgrid," *J. Modern Power Syst. Clean Energy*, vol. 11, no. 4, pp. 1–14, Jul. 2022.

[4] J. Pahasa, P. Potejana, and I. Ngamroo, "MPC-based virtual energy storage system using PV and air conditioner to emulate virtual inertia and frequency regulation of the low-inertia microgrid," *IEEE Access*, vol. 10, pp. 133708–133719, 2022.

[5] S. Muangchuen, J. Pahasa, and I. Ngamroo, "Improved resilient model predictive control for enhanced microgrid virtual inertia emulation by virtual energy storage system under DoS attacks," *IEEE Access*, vol. 11, pp. 96817–96830, 2023.

[6] M. G. Dozein, A. M. De Corato, and P. Mancarella, "Virtual inertia response and frequency control ancillary services from hydrogen electrolyzers," *IEEE Trans. Power Syst.*, vol. 38, no. 3, pp. 2447–2459, May 2023.

[7] M. B. Hossain, M. R. Islam, K. M. Muttaqi, D. Sutanto, and A. P. Agalgaonkar, "Power system dynamic performance analysis based on frequency control by proton exchange membrane electrolyzers," *IEEE Trans. Ind. Appl.*, vol. 59, no. 4, pp. 1–11, Aug. 2023.

[8] M. B. Hossain, M. R. Islam, K. M. Muttaqi, D. Sutanto, and A. P. Agalgaonkar, "Dynamic electrical circuit modeling of a proton exchange membrane electrolyzer for frequency stability, resiliency, and sensitivity analysis in a power grid," *IEEE Trans. Ind. Appl.*, vol. 59, no. 6, pp. 7271–7281, Dec. 2023.

[9] Á. Iribarren, D. Elizondo, E. L. Barrios, H. Ibaiondo, A. Sanchez-Ruiz, J. Arza, P. Sanchis, and A. Ursúa, "Dynamic modeling of a pressurized alkaline water electrolyzer: A multiphysics approach," *IEEE Trans. Ind. Appl.*, vol. 59, no. 3, pp. 1–11, May 2023.

[10] M. Chlela, D. Mascarella, G. Joós, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018.

[11] M. Jamali, H. R. Baghaee, M. S. Sadabadi, G. B. Gharehpetian, and A. Anvari-Moghaddam, "Distributed cooperative event-triggered control of cyber-physical AC microgrids subject to denial-of-service attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4467–4478, Nov. 2023.

[12] W. Yao, Y. Wang, Y. Xu, and C. Deng, "Cyber-resilient control of an islanded microgrid under latency attacks and random DoS attacks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5858–5869, Apr. 2023.

[13] S. Hu, X. Ge, X. Chen, and D. Yue, "Resilient load frequency control of islanded AC microgrids under concurrent false data injection and denial-of-service attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 690–700, Jan. 2023.

[14] S. Hu, X. Ge, Y. Li, X. Chen, X. Xie, and D. Yue, "Resilient load frequency control of multi-area power systems under DoS attacks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 936–947, 2023.

[15] Q. Sun, K. Zhang, and Y. Shi, "Resilient model predictive control of cyber–physical systems under DoS attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4920–4927, Jul. 2020.

[16] W. Liu, J. Sun, G. Wang, F. Bullo, and J. Chen, "Data-driven resilient predictive control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 68, no. 8, pp. 1–16, Aug. 2022.

[17] Y. Dai, M. Li, K. Zhang, and Y. Shi, "Robust and resilient distributed MPC for cyber-physical systems against DoS attacks," *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 1, no. 1, pp. 44–55, Jun. 2023.

[18] A. Bemporad, M. Morari, and N. L. Ricker, *Model Predictive Control Toolbox? User's Guide*. Natick, MA, USA: MathWorks Inc., 2019.

[19] M. J. Khojasteh, A. Khina, M. Franceschetti, and T. Javidi, "Learning-based attacks in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 437–449, Mar. 2021.

[20] Y. Zhang, C. Peng, S. Xie, and X. Du, "Deterministic network calculus-based H8 load frequency control of multiarea power systems under malicious DoS attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1542–1554, Mar. 2022.

SATAWAT MUANGCHUEN received the B.Eng. and M.Eng. degrees in electrical engineering from the University of Phayao, Phayao, Thailand, in 2010 and 2015, respectively, where he is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, School of Engineering.

His research interest includes power system load frequency control.

JONGLAK PAHASA (Member, IEEE) received the B.Eng. degree in electrical engineering from the King Mongkut's Institute of Technology Ladkrabang (KMITL), Bangkok, Thailand, in 1997, the M.Eng. degree in electrical engineering from Chiang Mai University, Chiang Mai, Thailand, in 2007, and the D.Eng. degree in electrical engineering from KMITL, in 2011.

She is currently an Associate Professor with the School of Engineering, University of Phayao, Phayao, Thailand. Her current research interests include the application of artificial intelligence to power system stability and control.

CHAWASAK RAKPENTHAI (Member, IEEE) received the B.Eng., M.Eng., and Ph.D. degrees in electrical engineering from Chiang Mai University, Chiang Mai, Thailand, in 1999, 2003, and 2007, respectively. He is currently an Associate Professor with the Department of Electrical Engineering, School of Engineering, University of Phayao, Phayao, Thailand. His research interests include applications of artificial intelligence in power systems, power electronics, power system state estimation, and FACTS devices.

APPENDIX D Proceedings EECON – 45

การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 45
The 45th Electrical Engineering Conference (EECON-45)
วันที่ 16-18 พฤศจิกายน 2565 ณ ภูสักธาร รีสอร์ท อำเภอเมือง จังหวัดเลยราชภัฏ

การควบคุมอินเวอร์เตอร์เครื่องปรับอากาศสำหรับเพิ่มแรงเฉื่อยเสมือนของไมโครกริด

Inverter Air Conditioner Control for Virtual Inertia Emulator of Microgrid

ศตวรรษ เมืองชื่น [1], อิสระชัย งามหรู [2] และ จงลักษณ์ พาทะชา [1,*]

[1]ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยพะเยา jonglak.pa@up.ac.th

[2]ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง issarachai.ng@kmitl.ac.th

บทคัดย่อ

การเพิ่มขึ้นของแหล่งจ่ายพลังงานทดแทน เช่น เครื่องกำเนิดไฟฟ้าพลังลม และเครื่องกำเนิดไฟฟ้าพลังแสงอาทิตย์ ซึ่งเชื่อมต่อระบบไฟฟ้ากำลังด้วยอุปกรณ์แปลงผันอิเล็กทรอนิกส์ ส่งผลให้ระบบไฟฟ้ากำลังมีความเฉื่อยลดลง ทำให้อัตราการเปลี่ยนแปลงของความถี่มีค่าสูงขึ้น ทำให้ระบบไฟฟ้ากำลังมีโอกาสเกิดไฟดับได้ง่ายขึ้น งานวิจัยนี้ นำเสนอการควบคุมอินเวอร์เตอร์ของเครื่องปรับอากาศเพื่อเพิ่มแรงเฉื่อยเสมือนของไมโครกริด ตัวควบคุมที่ใช้เป็นตัวควบคุม พีไอดี ที่หาค่าเหมาะสมที่สุดด้วยอัลกอริทึมหิ่งห้อย ผลการจำลองกับระบบไมโครกริดที่ทำการศึกษา พบว่า การควบคุมเครื่องปรับอากาศอินเวอร์เตอร์ที่ควบคุมด้วยพีไอดีที่เหมาะสมที่สุด สามารถเพิ่มแรงเฉื่อยเสมือนให้กับระบบไมโครกริดซึ่งดีกว่าการควบคุมพีไอดีแบบทั่วไป

คำสำคัญ: การควบคุมความถี่โหลด การควบคุมพีไอดีที่เหมาะสมที่สุด เครื่องปรับอากาศอินเวอร์เตอร์ ไมโครกริด อัลกอริทึมหิ่งห้อย

Abstract

The increasing of intermittent renewable energy resources, such as wind power and photovoltaic generations which are connected to the power system by electronic power converter, reduce the power system inertia and increase the rate of change of frequency. This paper proposes the application of inverter-air conditioner (IAC) control to improve the virtual inertia emulator. The controller used is a proportional integral derivative (PID) controller. The PID parameters are optimized by the firefly algorithm. Simulation results revealed that the IAC controlled by optimal PID is able to improve the virtual inertia of the studied microgrid when compared to the conventional PID controller.

Keywords: Load frequency control, optimal PID control, inverter air-conditioner, microgrid, firefly algorithm

1. บทนำ

การเพิ่มขึ้นของแหล่งจ่ายพลังงานทดแทน เช่น เครื่องกำเนิดไฟฟ้าพลังลม และเครื่องกำเนิดไฟฟ้าพลังแสงอาทิตย์ ซึ่งเชื่อมต่อระบบไฟฟ้ากำลังด้วยอุปกรณ์อิเล็กทรอนิกส์กำลัง เป็นสาเหตุหนึ่งที่ทำให้ระบบไฟฟ้าทำลังมีความเฉื่อยลดลง ซึ่งโดยปกติความเฉื่อยนี้ได้มาจากเครื่องกำเนิดไฟฟ้าชิงโครนัส [1-2] การเพิ่มแรงเฉื่อยเสมือนทำได้หลายวิธี ยกตัวอย่างเช่น การติดตั้งอุปกรณ์กักเก็บพลังงานเพื่อเพิ่มแรงเฉื่อยเสมือนให้กับระบบไมโครกริด [1-2] อย่างไรก็ตามอุปกรณ์กักเก็บพลังงานเช่น แบตเตอรี่มีข้อเสียคือ ต้องใช้เงินลงทุนในการซื้ออุปกรณ์กักเก็บพลังงาน และเมื่อหมดอายุการใช้งานก็ไม่สามารถกำจัดให้หมดไปได้ ดังนั้นการประยุกต์ใช้สมาร์ทโหลดเช่น เครื่องปรับอากาศอินเวอร์เตอร์ จึงเป็นอีกทางเลือกหนึ่งที่น่าสนใจ

นอกจากนี้ การเพิ่มขึ้นของอุณหภูมิทำให้จำนวนการใช้เครื่องปรับอากาศมีปริมาณเพิ่มมากขึ้นด้วย ซึ่งโดยปกติเครื่องปรับอากาศอินเวอร์เตอร์ถูกใช้เพื่อควบคุมอุณหภูมิห้องให้เท่ากับที่ผู้ใช้ตั้งไว้เพื่อความสบายของคนอาศัยในห้องนั้น ค่าที่แท้จริงของอุณหภูมิห้องเป็นสิ่งสำคัญ อย่างไรก็ตามสำหรับบางคนที่อาศัยอยู่ในอพาร์ทเม้น อาจไม่ได้สำคัญว่าอุณหภูมิห้องจะเบี่ยงเบนจากค่าที่ตั้งไว้เท่าไร ดังนั้น การควบคุมการเบี่ยงเบนของอุณหภูมิห้อง ซึ่งนี่คือ การควบคุมการใช้กำลังไฟฟ้าของเครื่องปรับอากาศอินเวอร์เตอร์ก็สามารถนำมาประยุกต์ใช้เพื่อช่วยในการควบคุมความถี่ระบบไฟฟ้ากำลังได้ [3] ซึ่งสามารถนำมาใช้เพื่อเพิ่มแรงเฉื่อยเสมือนในระบบไฟฟ้ากำลังได้ด้วยเช่นกัน ส่งผลให้อัตราการเปลี่ยนแปลงของความถี่ (rate of change of frequency: RoCoF) เมื่อเกิดการรบกวนในระบบลดลงด้วย

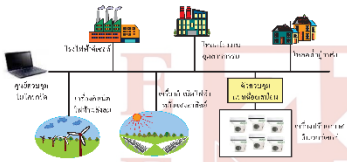
งานวิจัยนี้ นำเสนอการควบคุมอินเวอร์เตอร์ของเครื่องปรับอากาศเพื่อเพิ่มแรงเฉื่อยเสมือนของไมโครกริด ตัวควบคุมที่ใช้เป็นตัวควบคุมพีไอดี ที่หาค่าเหมาะสมที่สุดด้วยอัลกอริทึมหิ่งห้อย ผลการจำลองกับระบบไมโครกริด พบว่าการควบคุมเครื่องปรับอากาศอินเวอร์เตอร์ที่ควบคุมด้วยพีไอดีที่เหมาะสมที่สุด สามารถเพิ่มแรงเฉื่อยเสมือนให้กับระบบไมโครกริดได้ดีกว่าการควบคุมพีไอดีแบบทั่วไป

2. ระบบที่ใช้ในการศึกษา

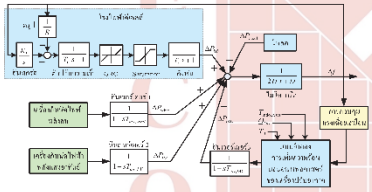
ระบบไมโครกริดที่ใช้ในการศึกษาแสดงดังรูปที่ 1 โดยระบบประกอบด้วย เครื่องกำเนิดไฟฟ้าดีเซลล์ขนาด 25 MW, เครื่องกำเนิดไฟฟ้าพลังแสงอาทิตย์ขนาด 10 MW, เครื่องกำเนิดไฟฟ้าพลังลมขนาด 12.5 MW, กลุ่มโหลดเครื่องปรับอากาศอินเวอร์เตอร์ขนาด 16 MW, และโหลดทั่วไปขนาด 20 MW [3] ค่าฐานของระบบคือ 20 MW จำนวน

การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 45
The 45th Electrical Engineering Conference (EECON-45)
วันที่ 16-18 พฤศจิกายน 2565 ณ ภูสักธาร รีสอร์ท อำเภอเมือง จังหวัดเลยเขาย

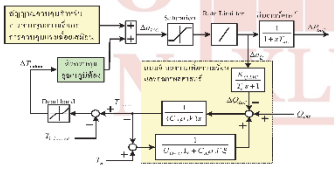
เครื่องปรับอากาศที่ใช้ทั้งหมด จำนวน 3,000 ลัว โดยแต่ละตัวมีขนาด 8 kW เนื่องจากการเปลี่ยนแปลงอย่างฉับพลันของกำลังไฟฟ้าจากเครื่องกำเนิดไฟฟ้าพลังแสงอาทิตย์และเครื่องกำเนิดไฟฟ้าพลังลม และการเปลี่ยนแปลงของโหลด ซึ่งทำให้เครื่องกำเนิดไฟฟ้าดีเซลล์ไม่สามารถชดเชยกำลังไฟฟ้าได้เพียงพอเนื่องจากการลอบสนองทางไดนามิกส์ช้า ดังนั้น การตอบสนองทางไดนามิกส์ที่เร็วของเครื่องปรับอากาศอินเวอร์เตอร์จึงได้ถูกนำมาใช้เพื่อชดเชยความไม่สมดุลของกำลังไฟฟ้าจริงในระบบด้วยการควบคุมการใช้กำลังไฟฟ้าของเครื่องปรับอากาศอินเวอร์เตอร์ [3] รูปที่ 2 แสดงแบบจำลองเชิงเส้นของไมโครกริดที่ใช้ในการศึกษา



รูปที่ 1 ไมโครกริดที่มีกลุ่มเครื่องปรับอากาศอินเวอร์เตอร์



รูปที่ 2 แบบจำลองเชิงเส้นของไมโครกริดที่ใช้ในการศึกษา



รูปที่ 3 แบบจำลองเชิงเส้นของกลุ่มเครื่องปรับอากาศอินเวอร์เตอร์

2.1 แบบจำลองเครื่องปรับอากาศอินเวอร์เตอร์

ในการประยุกต์ใช้เครื่องปรับอากาศอินเวอร์เตอร์เพื่อเพิ่มแรงเฉื่อยเสมือนให้กับไมโครกริด จะใช้แบบจำลองเครื่องปรับอากาศอินเวอร์เตอร์สำหรับใช้เพื่อควบคุมความถี่ [3] แสดงดังรูปที่ 3 โดยแบบจำลองเครื่องปรับอากาศอินเวอร์เตอร์ที่ใช้ในการจำลองประกอบด้วย 2 ส่วนคือ แบบจำลองคุณหภูมิห้อง และแบบจำลองไฟฟ้าของเครื่องปรับอากาศ [3]

(1) แบบจำลองอุณหภูมิห้อง คือแบบจำลองซึ่งอธิบายความสัมพันธ์ระหว่างอุณหภูมิห้องกับการเปลี่ยนแปลงความร้อนของห้องจากความจุความเย็น (refrigerating capacity) ของเครื่องปรับอากาศ โดยอุณหภูมิห้อง (T_{Indoor}) สามารถกำหนดเป็นดังสมการ

$$T_{Indoor} = \frac{Q_g - Q_{AC}}{C_A \rho_A V_R s} \tag{1}$$

$$Q_g = (U_{O,A} S_R + C_A \rho_A V_R \xi)(T_A - T_{Indoor}) + Q_{IN} \tag{2}$$

เมื่อ Q_g คือความร้อนที่เพิ่มขึ้นทั้งหมดของห้อง ที่มาจากการถ่ายเทความร้อนระหว่างอากาศภายในและภายนอกอาคาร, Q_{AC} คือความสามารถในการทำความเย็นของเครื่องปรับอากาศ, Q_{IN} คือการแผ่รังสีความร้อนจากสิ่งรบกวน เช่น คน หลอดไฟ และเครื่องใช้ต่างๆ, C_A คือความจุความร้อน, ρ_A คือความหนาแน่นของอากาศ, V_R คือปริมาตรของห้อง, S_R คือพื้นที่ผิวห้อง, s คือตัวแปรความถี่, T_A คืออุณหภูมิแวดล้อม, $U_{O,A}$ คือค่าสัมประสิทธิ์การถ่ายเทความร้อน และ ξ คือสัดส่วนการแลกเปลี่ยนอากาศระหว่างห้องกับบรรยากาศ

(2) แบบจำลองไฟฟ้าของเครื่องปรับอากาศ จะทำงานโดยใช้เครื่องปรับอากาศที่เชื่อมต่ออินเวอร์เตอร์ ทอมเพรสเซอร์ของเครื่องปรับอากาศสามารถเปลี่ยนความเร็วได้อย่างต่อเนื่องโดยการปรับความถี่ในการทำงาน กำลังไฟฟ้าที่เครื่องปรับอากาศใช้ไปและความสามารถในการทำความเย็นของเครื่องปรับอากาศถูกควบคุมด้วยความถี่ในการทำงานและสามารถแสดงดังสมการ

$$\Delta P_{AC} = \frac{K_P}{T_P s + 1} \Delta f_{AC} + \mu_P \tag{3}$$

$$\Delta Q_{AC} = \frac{K_Q}{T_Q s + 1} \Delta f_{AC} + \mu_Q \tag{4}$$

เมื่อ ΔP_{AC} คือ การเปลี่ยนแปลงของกำลังไฟฟ้าของเครื่องปรับอากาศจากกำลังไฟฟ้าอ้างอิงของเครื่องปรับอากาศ, ΔQ_{AC} คือ การเปลี่ยนแปลงของความจุการทำความเย็นของเครื่องปรับอากาศจากค่าอ้างอิง, Δf_{AC} คือการเปลี่ยนแปลงของความถี่ในการทำงานของเครื่องปรับอากาศจากความถี่อ้างอิง, K_P, K_Q, μ_P และ μ_Q คือค่าสัมประสิทธิ์คงที่ และ T_s คือค่าคงตัวเวลาของคอมเพรสเซอร์เครื่องปรับอากาศ

ความสัมพันธ์ระหว่างกำลังไฟฟ้าที่เครื่องปรับอากาศ P_{AC} และความสามารถในการทำความเย็น Q_{AC} สามารถแสดงได้ดังสมการ

$$Q_{AC} = \frac{K_Q}{K_P} P_{AC} + \frac{K_P \mu_Q - K_Q \mu_P}{K_P} \tag{5}$$

การเปลี่ยนแปลงความถี่ของเครื่องปรับอากาศอินเวอร์เตอร์นั้นขึ้นอยู่กับช่วงระหว่างค่าของอุณหภูมิที่ตั้งไว้กับอุณหภูมิห้องปัจจุบันเป็นหลัก และสามารถแสดงได้ดังสมการ

$$\Delta f_{AC} = K_1 \Delta T_{Indoor} \tag{6}$$

เมื่อ K_1 คือตัวควบคุมอุณหภูมิของเครื่องปรับอากาศ, ΔT_{Indoor} คือการเปลี่ยนแปลงระหว่างอุณหภูมิในห้องและอุณหภูมิที่ตั้งไว้

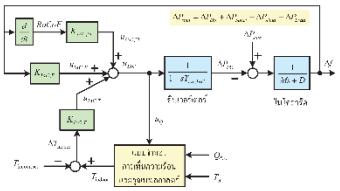
ถ้าใช้เครื่องปรับอากาศอินเวอร์เตอร์นี้ สำหรับช่วยควบคุมความถี่ จะทำให้ในการทำงานของเครื่องปรับอากาศอินเวอร์เตอร์ ก็จะได้รับอิทธิพลจากความถี่ของระบบด้วย ซึ่งสามารถอธิบายได้ดังสมการ

$$\Delta f_{AC} = K_1 \Delta T_{Indoor} + K_2 \Delta f \tag{7}$$

การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 45
The 45th Electrical Engineering Conference (EECON-45)
วันที่ 16-18 พฤศจิกายน 2565 ณ ภูสักธาร รีสอร์ท อำเภอเมือง จังหวัดเลยเขาย

เมื่อ K_v คือตัวควบคุมของเครื่องปรับอากาศสำหรับควบคุมความถี่

3. ตัวควบคุมที่นำเสนอ



รูปที่ 4 แบบจำลองเชิงเส้นของเครื่องปรับอากาศอินเวอร์เตอร์ที่เชื่อมต่อกับไมโครกริดสำหรับการควบคุมแรงเฉื่อยเสมือน

ดังแสดงในรูปที่ 4 ตัวควบคุมเครื่องปรับอากาศจำนวน 3 ตัวคือ $K_{IAC,1}$, $K_{IAC,1}$, และ $K_{IAC,2}$ ได้ถูกใช้เพื่อควบคุมแรงเฉื่อยเสมือน การเบี่ยงเบนความถี่ และอุณหภูมิห้อง ตามลำดับ อย่างไรก็ตาม เนื่องจากสัญญาณการเบี่ยงเบนความถี่เป็นอินพุตของ $K_{IAC,1}$ และ $K_{IAC,2}$ ดังนั้นงานวิจัยนี้จะใช้ตัวควบคุมพีไอดีจำนวน 2 ตัว ตามอินพุตที่มี 2 ตัว ทั้ง การเบี่ยงเบนของความถี่และการเบี่ยงเบนของอุณหภูมิ นั่นคือตัวควบคุมพีไอดีที่ใช้จึงสามารถแสดงเป็นสมการได้ดังต่อไปนี้

$$u_{IAC,F} = \left(K_{P,1} + \frac{K_{I,1}}{s} + K_{D,1} \right) \Delta f \tag{8}$$

$$u_{IAC,T} = \left(K_{P,2} + \frac{K_{I,2}}{s} + K_{D,2} \right) \Delta T_{Inhour} \tag{9}$$

$$u_{IAC} = u_{IAC,F} + u_{IAC,T} \tag{10}$$

งานวิจัยนี้จะใช้อัลกอริทึมหิ่งห้อย (Firefly algorithm: FA) [4] ทำการหาค่าพารามิเตอร์ของตัวควบคุมพีไอดีที่เหมาะสมที่สุด โดยวัตถุประสงค์ของการควบคุมคือ การหาค่าน้อยสุดของการเบี่ยงเบนความถี่ (Δf) และค่าน้อยสุดของการเบี่ยงเบนของอัตราการเปลี่ยนแปลงความถี่ ($\Delta RoCoF$) พร้อมทั้งรักษาการเบี่ยงเบนของอุณหภูมิห้องให้เปลี่ยนแปลงในช่วงที่ยอมรับได้ ปัญหาการหาค่าเหมาะสมสามารถตั้งสมการได้เป็น

$$\text{Minimize } J_c = \int_{t_{ini}}^{t_{end}} \left(w_1 \left| \Delta f(t) \right| + w_2 \left| \Delta RoCoF(t) \right| \right) dt \tag{11}$$

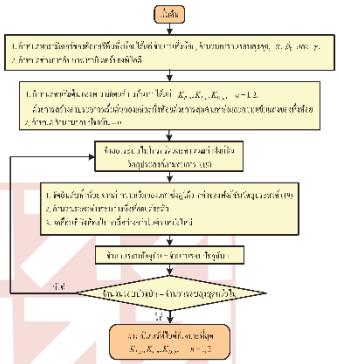
$$\text{Subject to } \Delta T_{Inhour}^{min} \le \Delta T_{Inhour}(t) \le \Delta T_{Inhour}^{max},$$

$$K_{P,n}^{min} \le K_{P,n} \le K_{P,n}^{max},\ K_{I,n}^{min} \le K_{I,n} \le K_{I,n}^{max},$$

$$K_{D,n}^{min} \le K_{D,n} \le K_{D,n}^{max}, \quad n = 1,2$$

เมื่อ w_1 และ w_2 คือ เวกเตอร์น้ำหนัก, t คือเวลาในการจำลอง, t_{ini} และ t_{end} คือเวลาเริ่มต้นและเวลาสิ้นสุดของการจำลอง ตามลำดับ, ΔT_{Inhour}^{min} และ ΔT_{Inhour}^{max} คือค่าการเบี่ยงเบนอุณหภูมิต่ำสุดและสูงสุดของการเบี่ยงเบนอุณหภูมิห้อง (ΔT_{Inhour}), $K_{P,n}^{min}$ และ $K_{P,n}^{max}$ คือพารามิเตอร์ต่ำสุดและสูงสุดของการค้นหาของ $K_{P,n}$, $K_{I,n}^{min}$ และ $K_{I,n}^{max}$ คือพารามิเตอร์ต่ำสุดและสูงสุดของการค้นหาของ $K_{I,n}$, $K_{D,n}^{min}$ และ $K_{D,n}^{max}$ ตามลำดับ

ขั้นตอนการทำงานของอัลกอริทึมหิ่งห้อยแสดงดังรูปที่ 5 สังเกตว่า α คือพารามิเตอร์ที่ได้จากการสุ่ม, β_0 คือความน่าดึงดูดในการวนซ้ำรอบที่ 0, และ γ คือค่าสัมประสิทธิ์การดูดกลืนแสงของอัลกอริทึมหิ่งห้อย [4]



รูปที่ 5 ขั้นตอนการหาพารามิเตอร์ที่เหมาะสมของอัลกอริทึมหิ่งห้อย

4. ผลการจำลอง

ระบบไมโครกริดดังรูปที่ 1-3 ถูกใช้เพื่อทดสอบวิธีที่นำเสนอ ด้วยโปรแกรม MATLAB/Simulink โดยพารามิเตอร์ของแบบจำลองเครื่องปรับอากาศ [3] มีดังนี้: $C_a = 1.005$ kJ/kg/°C, $\rho_a = 1.205$ kJ/m^3, $V_R = 250$ m^3, $S_R = 100$ m^2, $T_o = 35$ °C, $U_{o,A} = 3.6$ W/m^2/°C, $\xi = 0.5$ h^{-1} การหาค่าเหมาะสมของพารามิเตอร์ของตัวควบคุมพีไอดีช่วงของการเบี่ยงเบนของอุณหภูมิห้องตั้งค่าไว้ที่ ± 1 °C

พารามิเตอร์ของอัลกอริทึมหิ่งห้อยและพารามิเตอร์การค้นหา คือ จำนวนหิ่งห้อย = 20, จำนวนรอบการวนซ้ำสูงสุด = 100, $\alpha = 0.5$, $\beta_0 = 0.1$, และ $\gamma = 1$ เส้นโค้งการลู่เข้าของอัลกอริทึมหิ่งห้อยแสดงดังรูปที่ 6 พารามิเตอร์พีไอดีที่ได้คือ

$K_{P,1} = 443.719$, $K_{I,1} = 45.202$, $K_{D,1} = 4.008$,
$K_{P,2} = 0.512$, $K_{I,2} = 0.107$, $K_{D,2} = 0.036$

โดยในการจำลองจะสมมุติให้ (1) ทำการปลดเครื่องกำเนิดไฟฟ้าพลังลมที่เวลา 1,000 s ในกรณีนี้นั้นแหล่งจ่ายลดลง ดังนั้นเครื่องปรับอากาศจะต้องใช้กำลังไฟฟ้าลดลง ส่งผลให้อุณหภูมิห้องสูงกว่าค่าที่ตั้งไว้ (2) ทำการเชื่อมต่อเครื่องกำเนิดไฟฟ้าพลังลมที่เวลา 2,000 s ในกรณีนี้แหล่งจ่ายเพิ่มขึ้น ดังนั้นเครื่องปรับอากาศจะต้องใช้กำลังไฟฟ้าส่งผลให้อุณหภูมิห้องต่ำกว่าค่าที่ตั้งไว้

ผลการจำลองเปรียบเทียบระหว่างการไม่ใช้กลุ่มเครื่องปรับอากาศมาช่วยในการรักษาความถี่ (No-PFR), ตัวควบคุมพีไอดีทั่วไป (C-PID) และตัวควบคุมพีไอดีที่หาค่าเหมาะสมด้วยอัลกอริทึมหิ่งห้อย (FA-PID)

แสดงดังรูปที่ 7 โดยพารามิเตอร์ของการควบคุมด้วย C-PID แบบทั่วไปจะใช้คำสั่ง Tune ใน บล็อก PID ของโปรแกรม MATLAB/Simulink ซึ่งไม่ได้มีการนำค่า RoCoF ป้อนกลับในระบบมาใช้ พารามิเตอร์ที่ได้ คือ

$K_{P,1} = 195.312,\ K_{I,} = 39.481,\ K_{D,1} = 3.210,$

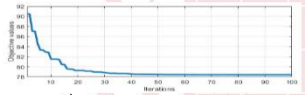
$K_{P,2} = 0.981,\quad K_{I,2} = 0.493,\ \ K_{D,2} = 0.072$

จากรูปที่ 7 จะเห็นว่า การควบคุมเครื่องปรับอากาศอินเวอร์เตอร์ที่ควบคุมด้วย FA-PID ให้การเปลี่ยนแปลงความถี่และอัตราการเปลี่ยนแปลงของความถี่ (RoCoF) ต่ำกว่า No-PFR และ C-PID ซึ่งแสดงให้เห็นว่ากลุ่มของเครื่องปรับอากาศสามารถเพิ่มแรงเฉื่อยเสมือนให้กับระบบไมโครกริดได้

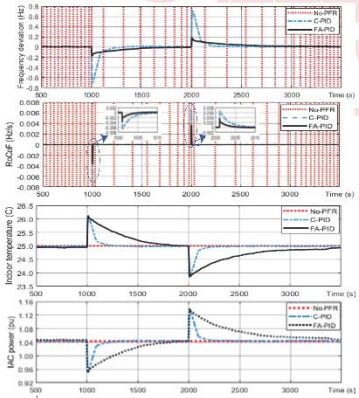
นอกจากนี้ จากรูปที่ 7 กำลังไฟฟ้าของเครื่องปรับอากาศ (IAC power) และอุณหภูมิห้องในกรณี C-PID และ FA-PID ไม่แตกต่างกันมากนักนั่นคือใช้กำลังไฟฟ้า ±0.01pu และอุณหภูมิมีการเปลี่ยนแปลงที่ ±1 °C ในช่วงมีการปลด/ต่อกลับเครื่องกำเนิดไฟฟ้าพลังลมขนาดกำลังไฟฟ้า 0.10 pu

รูปที่ 8 แสดงผลการจำลองเมื่อเปลี่ยนแปลงจำนวนเครื่องปรับอากาศ ซึ่งจะเห็นว่าเมื่อจำนวนเครื่องปรับอากาศมากขึ้นจะสามารถลดการแกว่งของความถี่ และลดอัตราการเปลี่ยนแปลงความถี่ได้

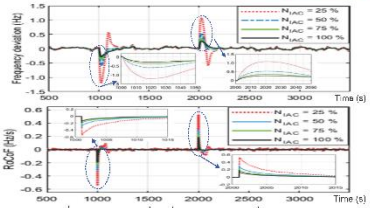
รูปที่ 9 แสดงผลการจำลองเมื่อมีการตั้งค่าอุณหภูมิห้องต่างๆ ซึ่งสามารถสรุปได้ว่า เมื่อจำนวนเครื่องปรับอากาศมากขึ้นจะทำให้สามารถลดการแกว่งของความถี่ และลดอัตราการเปลี่ยนแปลงความถี่ได้ดีกว่าจำนวนเครื่องปรับอากาศน้อยกว่า



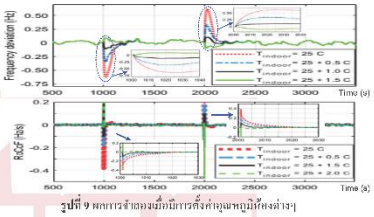
รูปที่ 6 เส้นโค้งการลู่เข้าของอัลกอริทึมหิ่งห้อย



รูปที่ 7 ผลการจำลองเปรียบเทียบระหว่าง No-PFR, C-PID และ FA-PID



รูปที่ 8 ผลการจำลองเมื่อจำนวนเครื่องปรับอากาศ



รูปที่ 9 ผลการจำลองเมื่อมีการตั้งค่าอุณหภูมิห้องต่างๆ

5. สรุป

งานวิจัยนี้ นำเสนอการควบคุมอินเวอร์เตอร์ของเครื่องปรับอากาศเพื่อเพิ่มแรงเฉื่อยเสมือนของไมโครกริด ตัวควบคุมที่ใช้เป็นตัวควบคุมพีไอดี ที่หาค่าเหมาะสมที่สุดด้วยอัลกอริทึมหิ่งห้อย ผลการจำลองกับระบบไมโครกริด ซึ่งประกอบด้วย เครื่องกำเนิดไฟฟ้าดีเซลล์ เครื่องกำเนิดไฟฟ้าพลังแสงอาทิตย์ เครื่องกำเนิดไฟฟ้าพลังลม โหลด และกลุ่มเครื่องปรับอากาศอินเวอร์เตอร์ พบว่า การควบคุมเครื่องปรับอากาศอินเวอร์เตอร์ที่ควบคุมด้วยพีไอดีที่เหมาะสมที่สุด สามารถเพิ่มแรงเฉื่อยเสมือนให้กับระบบไมโครกริดซึ่งดีกว่าการควบคุม พีไอดีแบบทั่วไป และการไม่มีการควบคุม

กิตติกรรมประกาศ

งานวิจัยนี้ได้รับทุนสนับสนุนจากสำนักงานการวิจัยแห่งชาติ (National Research Council of Thailand)

เอกสารอ้างอิง

[1] T. Kerdphol, et. al, "Enhanced virtual inertia control based on derivative technique to emulate simultaneous inertia and damping properties for microgrid frequency regulation," *IEEE Access*, vol. 7, pp. 14422-14433, 2019.

[2] P. Saxena, N. Singh and A. K. Pandey, "Self-regulated solar PV systems: replacing battery via virtual inertia reserve," *IEEE Trans. Ener. Conv.*, vol. 36, no. 3, pp. 2185-2194, Sept. 2021.

[3] J. Pahasa, P. Potejana, and I. Ngamroo, "Multi-objective decentralized model predictive control for inverter air conditioner control of indoor temperature and frequency stabilization in microgrid," *Energies*, vol. 14, no. 21 (6969), pp. 1-28, Oct. 2021.

[4] X. S. Yang, *Engineering optimisation: an introduction with metaheuristic applications*, Wiley, New Jersey, 2010.

APPENDIX E Proceedings EECON – 46

การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 46
The 46th Electrical Engineering Conference (EECON-46)
วันที่ 15-17 พฤศจิกายน 2566 ณ ตึวานำ พลาซ่า กระบี่ อำเภอเมือง จังหวัดกระบี่

การควบคุมยานยนต์ไฟฟ้าเพื่อเพิ่มแรงเฉื่อยเสมือนของไมโครกริดที่มีแรงเฉื่อยเสมือนต่ำ ภายใต้การโจมตีแบบปฏิเสธการให้บริการ ด้วยตัวควบคุมพีไอดีแบบยืดหยุ่น

Electric Vehicle Control for Improving Virtual Inertia of Low-Inertia Microgrid Under Denial-of-Service Attacks by Resilient PID Controller

คฑาวรรษ เมืองชื่น[1] วิภารัตน์ ช่มอาวุธ[2] เชวศักดิ์ รักเป็นไทย[3] และ จงลักษณ์ พาหะชา[4,*]

[1]สาขาวิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยพะเยา satawat.muangchuen@gmail.com
[2]สาขาวิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยพะเยา pangkoob.ee@gmail.com
[3]สาขาวิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยพะเยา chawasak.ra@up.ac.th
[4,*]สาขาวิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยพะเยา jonglak.pa@up.ac.th

บทคัดย่อ

บทความนี้ นำเสนอการควบคุมยานยนต์ไฟฟ้าเพื่อปรับปรุงแรงเฉื่อยเสมือนจริงในไมโครกริดที่มีแรงเฉื่อยต่ำ ภายใต้การโจมตีทางไซเบอร์ ได้แก่ การโจมตีโดยการปฏิเสธการให้บริการ โดยตัวควบคุมที่ใช้เป็นตัวควบคุมพีไอดีแบบยืดหยุ่น ซึ่งพิจารณาการโจมตีแบบปฏิเสธการให้บริการ ผลการจำลองกับระบบไมโครกริดที่ทำการศึกษา พบว่า การควบคุมยานยนต์ไฟฟ้าด้วยตัวควบคุมพีไอดีแบบยืดหยุ่นที่นำเสนอซึ่งพิจารณาการผลของการโจมตีแบบปฏิเสธการให้บริการ สามารถเพิ่มแรงเฉื่อยเสมือนให้กับระบบไมโครกริดได้ดีกว่าการควบคุมพีไอดีแบบทั่วไปที่ไม่พิจารณาผลของการโจมตีทางไซเบอร์

คำสำคัญ: ไมโครกริด, ยานยนต์ไฟฟ้า, การควบคุมแรงเฉื่อยเสมือนจริง, การโจมตีทางไซเบอร์, พีไอดีแบบยืดหยุ่น

Abstract

This paper proposes an electric vehicle control to improve virtual inertia of a low-inertia microgrid under cyber-attacks i.e., denial-of-service attacks, by the resilient PID controller which is designed by consider the DoS attack. Simulation results revealed that the electric vehicle controlled by the proposed resilient PID is able to improve the virtual inertia of the studied microgrid when compared to the conventional PID controller which is not considering cyber-attacks.

Keywords: Microgrid, electric vehicle, virtual inertia control, cyber-attacks, resilient PID

1. ข้อมูลทั่วไป

การเพิ่มขึ้นของแหล่งจ่ายพลังงานทดแทน เช่น เครื่องกำเนิดไฟฟ้าพลังแสงอาทิตย์ และโหลดอัจฉริยะ เช่น ยานยนต์ไฟฟ้า ซึ่งเชื่อมต่อระบบไฟฟ้ากำลังด้วยอุปกรณ์แปลงผันอิเล็กทรอนิกส์กำลัง ส่งผลให้ระบบไฟฟ้ากำลังมีแรงเฉื่อยต่ำ (low inertia) ทำให้อัตราการเปลี่ยนแปลงของความถี่มีค่าสูงขึ้น ส่งผลให้ระบบไฟฟ้ากำลังมีโอกาสเกิดไฟฟ้าดับได้ง่ายขึ้น [1] นอกจากนี้ ตามแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 13 (ปี พ.ศ. 2566-2570) ได้ระบุไว้ว่า ไทยเป็นฐานการผลิตยานยนต์ไฟฟ้าที่สำคัญของโลก ซึ่งจะทำให้ปริมาณยานยนต์ไฟฟ้าในประเทศมีเพิ่มมากขึ้น ส่งผลต่อการลดลงของแรงเฉื่อยในระบบไฟฟ้ากำลังด้วย อย่างไรก็ตาม การควบคุมการประจุแบตเตอรี่ของยานยนต์ไฟฟ้าสามารถนำมาใช้เพื่อเพิ่มแรงเฉื่อยเสมือนจริงให้กับระบบไฟฟ้ากำลังได้ ดังได้มีการนำเสนอใน [2] ทั้งนี้ การควบคุมแบบกระจายตัวของระบบไมโครกริดส่งผลให้การส่งผ่านข้อมูลเพื่อใช้ในการควบคุมระบบผลิตไฟฟ้าแบบกระจายตัว หรือ โหลดอัจฉริยะแบบกระจายตัว เช่น การควบคุมการประจุยานยนต์ไฟฟ้า ดังกล่าว มีความอ่อนไหวต่อการโจมตีทางไซเบอร์ (cyber-attack) เช่น การโจมตีโดยการฉีดข้อมูลเท็จ (false data injection attack: FDI) หรือการโจมตีโดยการปฏิเสธการให้บริการ (denial of service attack: DoS) เป็นต้น [3]

บทความนี้ นำเสนอการควบคุมการประจุแบตเตอรี่ยานยนต์ไฟฟ้าเพื่อปรับปรุงแรงเฉื่อยเสมือนจริงในไมโครกริดภายใต้การโจมตีทางไซเบอร์ โดยมุ่งเน้นไปที่การโจมตีโดยการปฏิเสธการให้บริการ โดยตัวควบคุมที่ใช้จะเป็นตัวควบคุมพีไอดี (proportional integral derivative: PID) ที่มีการพิจารณาความเสียหายจากการถูกโจมตีทางไซเบอร์เปรียบเทียบกับตัวควบคุมพีไอดีที่ไม่มีการพิจารณาการโจมตีทางไซเบอร์

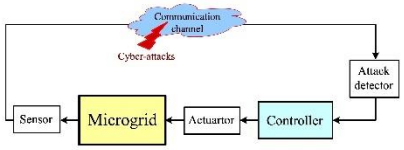
2. การกำหนดปัญหาและแบบจำลองที่ใช้

2.1 การควบคุมไมโครกริดภายใต้การโจมตีทางไซเบอร์

ในการควบคุมแบบกระจายตัวของไมโครกริด ตัวควบคุมจะถูกวางไว้ใกล้กับอุปกรณ์ต่างๆ แบบกระจายตัว เช่น เครื่องกำเนิดไฟฟ้ากังหันลม เครื่องกำเนิดไฟฟ้าเซลล์แสงอาทิตย์ และโหลดอัจฉริยะ เช่นยานยนต์ไฟฟ้า ประสิทธิภาพแบบไดนามิกส์ของไมโครกริดสามารถปรับปรุงได้อย่างมีนัยสำคัญโดยสัญญาณที่ส่งจากเซ็นเซอร์ไปยังตัวควบคุมแบบกระจายตัว อย่างไรก็ตาม การโจมตีทางไซเบอร์นั้นแพร่หลายใน

โครงข่ายการสื่อสารและส่งผลกระทบอย่างมากต่อความมีเสถียรภาพการทำงาน และการควบคุม ของไมโครกริด

รูปที่ 1 แสดงการควบคุมไมโครกริดภายใต้การโจมตีทางไซเบอร์ การโจมตีทางไซเบอร์จะเกิดขึ้นในช่องทางการสื่อสารระหว่างบล็อกตัวตรวจรู้ (Sensor) และตัวควบคุม (Controller) การโจมตีทางไซเบอร์จะทำความเสียหายให้กับการดำเนินงานของระบบด้วยการยกเลิกการบริการการสื่อสาร [3] ซึ่งอาจทำให้ประสิทธิภาพของตัวควบคุมลดลงระหว่างการโจมตีของ DoS ในความหมายนี้ บล็อกตัวควบคุม (Controller) ควรได้รับการออกแบบเพื่อลดผลกระทบจากสัญญาณการสื่อสารที่ขาดหายไปที่เป็นผลมากจากการโจมตีแบบ DoS



รูปที่ 1 การควบคุมไมโครกริดภายใต้การโจมตีทางไซเบอร์

2.2 การควบคุมแรงเฉื่อยเสมือนจริงในระบบไฟฟ้ากำลัง

โดยปกติแรงเฉื่อยในระบบไฟฟ้ากำลัง คือมวลหมุน (rotating mass) ของเครื่องกำเนิดไฟฟ้าซิงโครนัส ซึ่งทำการเชื่อมต่อแบบซิงโครนัสกับโครงข่ายระบบไฟฟ้ากำลัง ความเร็วของมวลหมุนจะเปลี่ยนไปเมื่อความต้องการใช้ไฟฟ้ามากกว่าการผลิตไฟฟ้าได้ ณ ช่วงเวลาใดก็ตาม จำนวนเครื่องกำเนิดไฟฟ้าแบบกระจายตัวที่ใช้สำหรับพลังงานทดแทนที่เพิ่มขึ้นในปัจจุบัน ซึ่งเครื่องกำเนิดไฟฟ้าแบบกระจายตัวดังกล่าว ทำการเชื่อมต่อกับโครงข่ายระบบไฟฟ้ากำลัง ผ่านอินเวอร์เตอร์อิเล็กทรอนิกส์กำลัง ซึ่งมีแรงเฉื่อยน้อย ทำให้แรงเฉื่อยของระบบไฟฟ้าลดลง การเพิ่มแรงเฉื่อยเสมือนด้วยการควบคุมกำลังไฟฟ้าจากอินเวอร์เตอร์เป็นอีกทางเลือกหนึ่งที่น่าสนใจในการเพิ่มแรงเฉื่อยของระบบไฟฟ้ากำลังสมัยใหม่ที่มีปริมาณสัดส่วนของพลังงานหมุนเวียนที่เชื่อมต่อกับระบบไฟฟ้ากำลังด้วยอินเวอร์เตอร์เพิ่มมากขึ้น นอกจากนี้ สมาร์ทโหลด (smart load) หรือโหลดอัจฉริยะ เช่น ยานยนต์ไฟฟ้าที่เชื่อมต่อกับกริดการไฟฟ้าผ่านอินเวอร์เตอร์ ก็สามารถใช้จำลองแรงเฉื่อยเสมือนได้ [2]

ดังอธิบายใน [1] อินเวอร์เตอร์อิเล็กทรอนิกส์กำลังถูกใช้เพื่อจำลองสมการการแกว่งของเครื่องกำเนิดไฟฟ้าแบบซิงโครนัสเพื่อใช้ในการควบคุมแรงเฉื่อยเสมือนจริง สมการการแกว่งของเครื่องกำเนิดไฟฟ้าแบบซิงโครนัส สามารถแสดงได้ดังสมการ

$$\bar{P}_m - \bar{P}_e = \frac{2H}{\omega_0}\frac{d^2\delta}{dt^2} = \frac{2H}{\omega_0}\frac{d\Delta\omega_r}{dt} \quad (1)$$

เมื่อ $\bar{P}_m$ คือ กำลังทางกลของเครื่องกำเนิดไฟฟ้าซิงโครนัส, $\bar{P}_e$ คือ กำลังทางไฟฟ้าของเครื่องกำเนิดไฟฟ้าซิงโครนัส, H คือ ค่าคงตัวแรงเฉื่อย, ω_0 คือ ความเร็วเชิงมุมพิกัดของโรเตอร์, ω_r คือ ความเร็วเชิงมุมของโรเตอร์, δ คือ มุมโรเตอร์ และ t คือ เวลา

เมื่อรวมส่วนประกอบการหน่วงที่มีสัมประสิทธิ์การหน่วง (damping coefficient: K_D) รวมอยู่ด้วย สมการ (1) สามารถเขียนได้ดังนี้

$$\bar{P}_m - \bar{P}_e = \frac{2H}{\omega_0}\frac{d\Delta\omega_r}{dt} + K_D\frac{\Delta\omega_r}{\omega_0} \quad (2)$$

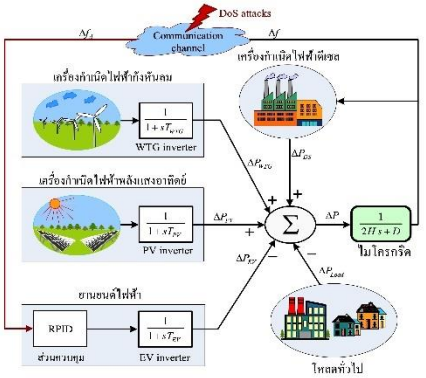
สำหรับปัญหาการควบคุมความถี่โหลด (load frequency control: LFC) การเบี่ยงเบนของความเร็วเชิงมุม (angular velocity deviation: $\Delta\omega_r$) จะเปลี่ยนแปลงตามการเบี่ยงเบนของความถี่ (frequency deviation: Δf) ดังนั้น สมการ (2) จึงสามารถเขียนใหม่ได้เป็นดังสมการ

$$\bar{P}_m - \bar{P}_e = \frac{2H}{f_0}\frac{d\Delta f}{dt} + K_D\frac{\Delta f}{f_0} \quad (3)$$

เมื่อ f_0 คือ ความถี่พิกัด, f คือ ความถี่ของระบบไฟฟ้ากำลัง, $d\Delta f/dt$ คือ อัตราการเบี่ยงเบนของความถี่ (rate of change of frequency: RoCoF)

2.3 แบบจำลองไมโครกริดสำหรับการควบคุมแรงเฉื่อยเสมือนจริง

รูปที่ 2 แสดงตัวอย่างการควบคุมแรงเฉื่อยเสมือนจริงของระบบไมโครกริด ด้วยยานยนต์ไฟฟ้า เมื่อมีสัญญาณการโจมตีทางไซเบอร์แบบ DoS โดยความแตกต่างระหว่างกำลังไฟฟ้าที่ผลิตขึ้น และความต้องการของโหลด ทำให้เกิดการเบี่ยงเบนของความถี่ออกจากความถี่ที่ระบุของระบบ (50 Hz หรือ 60 Hz) ถ้ากำลังไฟฟ้าที่ผลิตขึ้นน้อยกว่าความต้องการของโหลด จะทำให้ ความเร็วและความถี่ของเครื่องกำเนิดไฟฟ้าจะเริ่มลดลง หรือในทางกลับกัน ถ้ากำลังไฟฟ้าที่ผลิตขึ้นมากกว่าความต้องการของโหลด จะทำให้ ความเร็วและความถี่ของหน่วยเครื่องกำเนิดไฟฟ้าจะเริ่มเพิ่มขึ้น



รูปที่ 2 การควบคุมแรงเฉื่อยเสมือนในไมโครกริดเมื่อมีการโจมตี DoS

โดยการเบี่ยงเบนของความถี่ของไมโครกริด (Δf) สามารถเขียนได้ดังสมการดังต่อไปนี้

$$\Delta f = \frac{1}{2Hs+D}\left(\underbrace{\Delta P_{DS}+\Delta P_{PV}+\Delta P_{WTG}}_{\text{generated power}} \underbrace{-\Delta P_{Load}-\Delta P_{EV}}_{\text{demanded power}}\right) \quad (4)$$

เมื่อ H คือ คุณลักษณะแรงเฉื่อย, D คือ คุณลักษณะการหน่วง (damping), ΔP_{DS} คือ การเบี่ยงเบนกำลังไฟฟ้าของเครื่องกำเนิดไฟฟ้า

การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 46
The 46th Electrical Engineering Conference (EECON-46)
วันที่ 15-17 พฤศจิกายน 2566 ณ ดีวาน่า พลาซ่า กระบี่ อำเภอเมือง จังหวัดกระบี่

ดีเซล, ΔP_{PV} คือ การเบี่ยงเบนกำลังไฟฟ้าของเครื่องกำเนิดไฟฟ้าพลังแสงอาทิตย์, ΔP_{WTG} คือ การเบี่ยงเบนกำลังไฟฟ้าของเครื่องกำเนิดไฟฟ้าพลังลม, ΔP_{Load} คือ การเบี่ยงเบนกำลังไฟฟ้าของความต้องการของโหลด และ ΔP_{EV} คือ การเบี่ยงเบนกำลังไฟฟ้าของยานยนต์ไฟฟ้า

อัตราการเปลี่ยนแปลงของความถี่หรือ *RoCoF* ของไมโครกริดสามารถกำหนดได้เป็นดังสมการ

$$R=\frac{d\Delta f}{dt}=\frac{\Delta f(t)-\Delta f(t_p)}{t-t_p},\ t>t_p \tag{5}$$

เมื่อ R คือ สัญลักษณ์แบบสั้นของ *RoCoF*, t คือ เวลาปัจจุบันของการจำลอง, t_p คือ เวลาก่อนหน้าของการจำลอง (previous simulation times), $\Delta f(t)$ คือ การเบี่ยงเบนของความถี่ที่เวลาปัจจุบัน, และ $\Delta f(t_p)$ คือ การเบี่ยงเบนของความถี่ที่เวลาก่อนหน้า

3. แบบจำลองการโจมตีทางไซเบอร์แบบ DoS

หนึ่งในข้อกังวลด้านความปลอดภัยที่ร้ายแรงที่สุดสำหรับระบบไซเบอร์-กายภาพ (cyber-physical systems) คือการโจมตีแบบปฏิเสธการให้บริการ (denial of service: DoS) [3] เพื่อครอบครองหรือใช้ทรัพยากรที่จำกัด การโจมตีแบบ DoS จะส่งข้อมูลที่ทำให้เข้าใจผิดและไม่มีความหมายไปยังส่วนประกอบของระบบไฟฟ้า [3] ช่วงเวลาเหตุการณ์การโจมตีแบบ DoS สามารถระบุได้โดยสมการต่อไปนี้

$$\Im(0,\infty)\triangleq\bigcup_{l\in\mathbb{N}}[T_{on,l},T_{off,l}] \tag{6}$$

เมื่อ T คือ ช่วงเวลาการชักตัวอย่าง, $T_{on,l}\in[T_{on}^{\min},T],l\in\mathbb{N}$ คือ เวลาที่เกิดการโจมตีแบบ DoS ครั้งแรก หรือเวลาเริ่มเกิดการโจมตี, $T_{off,l}\in[T_{off}^{\min},T],l\in\mathbb{N}$ คือ ช่วงเวลาที่การโจมตีแบบ DoS สิ้นสุดลง, $T_{on}<T_{off}\le T$ คือ เวลาทริกเกอร์ (trigger time) สำหรับการโจมตีแบบ DoS แต่ละครั้ง, และ $T_{off}-T_{on}$, คือ ระยะเวลาการโจมตี

แบบจำลองของการโจมตีแบบ DoS แบบตัวแปรสุ่มไม่เป็นรายคาบในช่วงเวลาเกิด DoS ทั้งหมดสามารถกำหนดได้ดังสมการ

$$S_{DoS}(t)=\begin{cases}0, & t\in\Im(0,\infty)\\ 1, & t\notin\Im(0,\infty)\end{cases} \tag{7}$$

เมื่อ $S=0$ คือ การเกิดขึ้นของการโจมตีแบบ DoS และ $S=1$ คือ การส่งสัญญาณปกติ

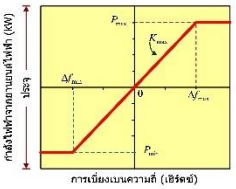
4. RPID สำหรับการควบคุมแรงเฉื่อยเสมือนจริงด้วยยานยนต์ไฟฟ้าภายใต้การโจมตีแบบ DoS

รูปที่ 3 แสดงการควบคุมกำลังไฟฟ้าของยานยนต์ไฟฟ้าต่อการเปลี่ยนแปลงความถี่ [4] ซึ่งจะเห็นว่าการควบคุมการประจุแบตเตอรี่ของยานยนต์ไฟฟ้าสามารถนำมาใช้เพื่อลดการเบี่ยงเบนของความถี่ในระบบไมโครกริด ซึ่งเกิดจากความไม่แน่นอนของแหล่งจ่ายพลังลมและแหล่งจ่ายพลังแสงอาทิตย์ ที่ผู้วิจัยได้นำเสนอไว่ในงานวิจัย [4] นอกจากนี้ การประจุแบตเตอรี่ยานยนต์ไฟฟ้ายังสามารถนำมาใช้เพื่อเพิ่มแรงเฉื่อยเสมือนจริงให้กับระบบไฟฟ้ากำลังได้ ดังมีการนำเสนอในงานวิจัย [2] รูปที่ 4 แสดงแบบจำลองยานยนต์ไฟฟ้าสำหรับควบคุมแรงเฉื่อยเสมือนจริงด้วยตัวควบคุมพีไอดีแบบยืดหยุ่น (resilient PID: RPID) ที่นำเสนอ โดยเมื่อสัญญาณการเบี่ยงเบนความถี่ (Δf) ได้รับความเสียหายจากการโจมตีแบบ DoS ทำให้สัญญาณ $\Delta f=0$ ซึ่งหากใช้สัญญาณนี้ในการควบคุมกำลังไฟฟ้าของยานยนต์ไฟฟ้าก็อาจทำให้เกิดความเสียหายได้ ดังนั้น เพื่อแก้ปัญหาดังกล่าว สัญญาณควบคุมยานยนต์ไฟฟ้า สำหรับ RPID จึงสามารถเขียนได้เป็น

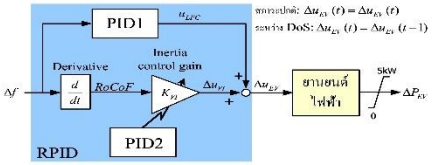
$$\Delta u_{EV}(t)=\begin{cases}\Delta u_{EV}(t-1), & During\ DoS\\ \Delta u_{EV}(t), & Otherwise\end{cases} \tag{8}$$

5. ผลการจำลอง

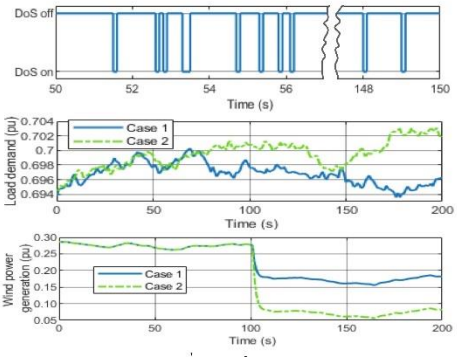
รูปที่ 5 แสดงกรณีศึกษา ซึ่งประกอบด้วยสัญญาณการโจมตีทางไซเบอร์แบบ DoS ในช่วงเวลา 50 s ถึง 150 s ความต้องการของโหลดทั่วไป 2 กรณี โดยกรณี 1 มีการเปลี่ยนแปลงของโหลดน้อยกว่ากรณี 2 และกำลังไฟฟ้าจากเครื่องกำเนิดไฟฟ้าพลังลม ซึ่งมีการปลดเครื่องกำเนิดไฟฟ้าพลังลมออกที่เวลา 100 s ขนาด 0.10 pu สำหรับกรณี 1 และ 0.2 pu สำหรับกรณี 2 ซึ่งจะเห็นว่าเป็นการปลดเครื่องกำเนิดไฟฟ้าระหว่างมีการโจมตีแบบ DoS



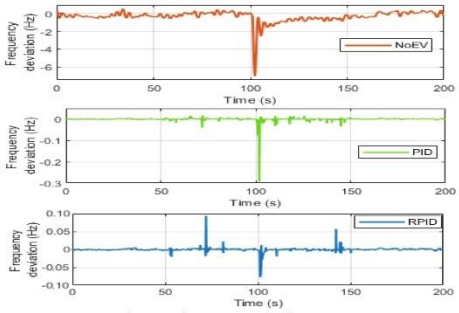
รูปที่ 3 การควบคุมกำลังไฟฟ้าของ EV ต่อการเปลี่ยนแปลงความถี่



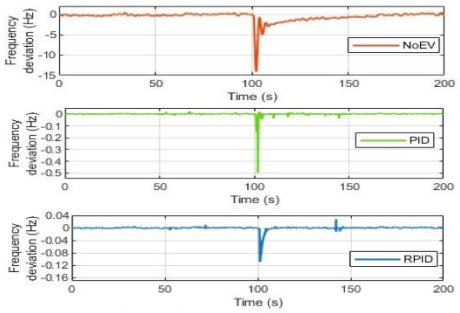
รูปที่ 4 แบบจำลองยานยนต์ไฟฟ้าเพื่อควบคุมแรงเฉื่อยเสมือนจริง



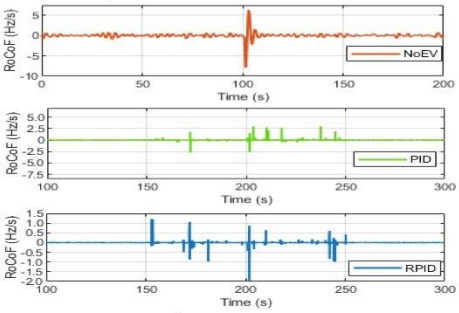
รูปที่ 5 กรณีศึกษา



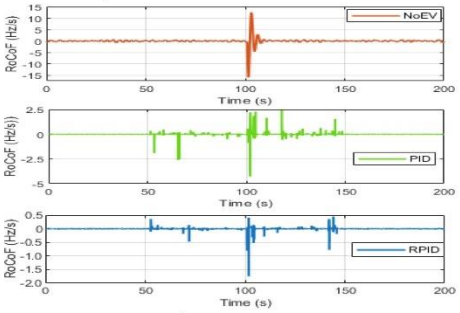
รูปที่ 6 การเบี่ยงเบนของความถี่ กรณี 1



รูปที่ 8 การเบี่ยงเบนของความถี่ กรณี 2



รูปที่ 7 RoCoF กรณี 1



รูปที่ 9 RoCoF กรณี 2

โดยวิธีนำเสนอจะเปรียบเทียบกับ อีก 2 วิธีคือ NoEV และ PID โดยวิธี NoEV คือ ระบบไมโครกริดที่ไม่ใช้ EV ในการเพิ่มแรงเฉื่อยเสมือน และ PID คือ การใช้ EV เพื่อเพิ่มแรงเฉื่อยเสมือนดังรูปที่ 4 แต่ไม่มีการเปลี่ยนแปลงสัญญาณควบคุม EV นั่น คือ $\Delta u_{EV}(t) = \Delta u_{EV}(t)$ เสมอ

ผลการจำลองกรณี 1 แสดงดังรูปที่ 6-7 โดยรูปที่ 6 แสดงการเบี่ยงเบนความถี่ของทั้งสามกรณีที่นำมาเปรียบเทียบ ซึ่งพบว่า การเบี่ยงเบนของความถี่ในกรณี RPID ที่นำเสนอต่ำกว่าวิธี PID และ NoEV อย่างชัดเจน โดยสังเกตจากค่ามากที่สุดบนแกนตั้งที่แสดงถึงการเบี่ยงเบนความถี่ รูปที่ 7 แสดง RoCoF ของทั้งสามวิธีที่นำมาเปรียบเทียบ ซึ่งจะเห็นว่า วิธีนำเสนอ RPID ให้ค่า RoCoF ต่ำกว่า PID และ NoEV ซึ่งแสดงให้เห็นว่า วิธีการนำเสนอ RPID สามารถเพิ่มแรงเฉื่อยเสมือนให้กับระบบไมโครกริดได้ดีกว่า วิธี PID และ NoEV

ผลการจำลองกรณี 2 แสดงดังรูปที่ 8-9 โดยรูปที่ 8 แสดงการเบี่ยงเบนความถี่ของทั้งสามกรณีที่นำมาเปรียบเทียบ ซึ่งพบว่า การเบี่ยงเบนของความถี่ในกรณี RPID ที่นำเสนอต่ำกว่าวิธี PID และ NoEV อย่างชัดเจน โดยสังเกตจากค่ามากที่สุดบนแกนตั้งที่แสดงถึงการเบี่ยงเบนของความถี่ รูปที่ 9 แสดง RoCoF ของทั้งสามวิธีที่นำมาเปรียบเทียบ ซึ่งจะเห็นว่าวิธีนำเสนอ RPID สามารถเพิ่มแรงเฉื่อยเสมือนให้กับระบบไมโครกริดได้ดีกว่า วิธี PID และ NoEV

6. สรุปผล

บทความนี้ นำเสนอการควบคุมยานยนต์ไฟฟ้าเพื่อปรับปรุงแรงเฉื่อยเสมือนในไมโครกริดภายใต้การโจมตีทางไซเบอร์แบบ DoS โดยตัวควบคุมที่ใช้เป็นควบคุมพีไอดีแบบยืดหยุ่น (RPID) ผลการจำลองกับระบบที่ทำการศึกษา พบว่า การควบคุมยานยนต์ไฟฟ้าด้วยตัวควบคุม RPID ที่นำเสนอ สามารถเพิ่มแรงเฉื่อยเสมือนให้กับระบบไมโครกริดได้ เมื่อมีการโจมตีแบบ DoS และดีกว่าการควบคุมพีไอดีทั่วไปที่ไม่พิจารณาการโจมตีทางไซเบอร์

เอกสารอ้างอิง

[1] T. Kerdphol, et.al., *Virtual Inertia Synthesis and Control*, (Power Systems) 1st ed. Springer, 2021.

[2] G. Magdy, H. Ali and D. Xu, "Effective control of smart hybrid power systems: cooperation of robust LFC and virtual inertia control systems," *CSEE J. Pow. Ener. Syst.*, vol. 8, no. 6, pp. 1583-93, 2022.

[3] M. Jamali, et.al., "Distributed cooperative event-triggered control of cyber-physical AC microgrids subject to denial-of-service attacks," *IEEE Trans. Smart Grid.* (Early Access Article)

[4] J. Pahasa and I. Ngamroo, "PHEVs bidirectional charging/discharging and SoC control for microgrid frequency stabilization using multiple MPC," *IEEE Trans. Smart Grid*, vol.6, no.3, pp.526-533, 2015.

APPENDIX F Proceedings Phayao Research Conference 13

การประชุมวิชาการระดับชาติ พะเยาวิจัย ครั้งที่ 13
PHAYAO RESEARCH CONFERENCE
695

ความปลอดภัยทางไซเบอร์ของไมโครกริด

Cyber Attacks of Microgrid

ศตวรรษ เมืองชื่น[1*] และ จงลักษณ์ พาหะซา[1]
Satawat Muangchuen[1*] and Jonglak Pahasa[1]

บทคัดย่อ

ความสำคัญของการพิจารณาความปลอดภัยของไมโครกริดกำลังมีความสำคัญมากขึ้น เนื่องจากการเชื่อมต่อของไมโครกริดมีช่องโหว่ทางไซเบอร์ที่เกิดขึ้นจากการเปลี่ยนผ่านสู่ดิจิทัล และการพึ่งพาระบบเทคโนโลยีสารสนเทศ และการสื่อสาร (Information and Communications Technology : ICT) ที่เพิ่มมากขึ้น โดยเฉพาะอย่างยิ่งในปัจจุบันที่มีไมโครกริดเริ่มเข้ามามีบทบาทที่เพิ่มขึ้นในการสร้างไมโครกริดที่จะเกิดขึ้นในอนาคต บทความนี้กล่าวถึงแนวทางที่มีอยู่ที่เกี่ยวข้องกับความปลอดภัยที่จะถูกโจมตีทางไซเบอร์ในระบบไฟฟ้า จากมุมมองของไมโครกริด ในขั้นแรก เริ่มต้นด้วยการทบทวนเชิงพรรณนาโดยย่อของคำศัพท์ที่ใช้บ่อยที่สุดในวรรณกรรมที่เกี่ยวข้องล่าสุด ตามด้วยการนำเสนอความพยายามในการศึกษาไมโครกริดล่าสุดที่ได้รับการเผยแพร่เพื่อช่วยให้กำหนดทิศทางการวิจัยในอนาคตที่เหมาะสมจากหลายสาขา

คำสำคัญ: ความปลอดภัยทางไซเบอร์, ไมโครกริด, การโจมตีทางไซเบอร์

Abstract

The importance of microgrid security considerations is becoming increasingly important. This is because microgrid connections are subject to cyber vulnerabilities arising from digital transformation and increased reliance on information and communications technology (ICT) systems. Especially now that microgrids are starting to play an increasing role in building the microgrid that will occur in the future. This article discusses existing guidelines regarding security against cyberattacks in power systems from the perspective of a microgrid system. The first step begins with a brief descriptive review of the most frequently used terms in the recent relevant literature. This is followed by a presentation of recent published microgrid study efforts to help determine appropriate future research directions from many fields.

Keywords: cyber security, microgrid, cyber-attacks

[1] คณะวิศวกรรมศาสตร์ มหาวิทยาลัยพะเยา จังหวัดพะเยา 56000
[1] School of Engineering, University of Phayao, Phayao, 56000
* Corresponding author e-mail: Satawat.Muangchuen@gmail.com

บทนำ

ความมั่นคงในระบบไฟฟ้าไม่เพียงมีแค่เรื่องระบบการผลิต ส่ง จ่ายเท่านั้น ยังเกี่ยวข้องกับการสื่อสารของอุปกรณ์ในระบบ เพื่อให้ระบบมีความสมดุลระหว่างระบบการผลิต และโหลด นอกจากนี้ยังต้องคำนึงถึงคุณภาพทางไฟฟ้าด้วย ซึ่งความปลอดภัยทางไซเบอร์ก็เป็นสิ่งสำคัญ เนื่องจากเมื่อเทคโนโลยีถูกประยุกต์ใช้มากขึ้น และในไมโครกริดมีความซับซ้อนของภาคพลังงานเพิ่มขึ้น จึงได้มีการปรับปรุงโครงข่ายไฟฟ้าให้ทันต่อการขยายตัวของโหลด และพัฒนาระบบให้เกิดความสมาร์ทขึ้นอย่างมีนัยสำคัญ

การส่งจ่ายพลังงานแบบสองทิศทาง และการติดตามการเปลี่ยนแปลงพลังงานไฟฟ้าโดยอุปกรณ์ประเภทต่างๆ ภายในไมโครกริดเป็นขั้นตอนที่สำคัญในการปรับปรุงระบบไฟฟ้าให้มีประสิทธิภาพ การบริหารจัดการทรัพยากรหมุนเวียน ร่วมกับเทคโนโลยีการจัดการแบบกระจายอัจฉริยะ [1,2] เป็นส่วนสำคัญที่ช่วยให้ระบบสามารถรองรับเทคโนโลยีที่เจริญเติบโตอย่างรวดเร็วในอนาคต [1,2] ไมโครกริดสามารถลดต้นทุนการดำเนินงานและความสูญเสียทางไฟฟ้า โดยการกำหนดราคาตามเวลา [3] การพยากรณ์ความต้องการไฟฟ้า และราคาค่าไฟฟ้าจึงเป็นเครื่องมือสำคัญในการตัดสินใจของผู้ให้บริการพลังงาน ไมโครกริดยังมีความซับซ้อนของในการจัดการโครงข่ายพลังงาน มีความท้าทายในการจัดการข้อมูลของระบบการสื่อสาร และจะต้องรองรับกับแนวโน้มการสื่อสารแบบใหม่ ที่มีการประยุกต์ใช้อุปกรณ์อัจฉริยะมากขึ้น และการประยุกต์ยังต้องรองรับกับระบบงานเดิมที่ใช้งานกันอยู่ (legacy systems) [4] และที่สำคัญต้องมีการป้องกันการโจมตีทางไซเบอร์ [5]

การพัฒนาไมโครกริดเริ่มเมื่อปี 2005 ในทวีปยุโรป ได้กำหนดแผนพัฒนาเทคโนโลยีไมโครกริดในปี 2020 [2] นอกจากนี้ยังมีอีกหลายๆ โครงการที่ได้พัฒนาพื้นที่ทดสอบไมโครกริด เพื่อเพิ่มศักยภาพที่เกี่ยวข้องกับการเปลี่ยนแปลงของระบบนี้ ยังมีรายละเอียดทางเทคนิคในแต่ละโครงสร้างระบบที่แตกต่างกัน รวมถึงผลกระทบทางด้านสังคม และเศรษฐศาสตร์ ยังคงเป็นเรื่องที่ต้องให้ความสำคัญต่อไป [6] แนวทางในการเรียนรู้ และแก้ไขปัญหาในการพัฒนาไมโครกริด เน้นการประสานงานของโครงข่าย พร้อมกับรักษาเสถียรภาพของไมโครกริด ในอนาคตจะเป็นการรวมตัวของไมโครกริดหลายตัวเข้าด้วยกัน เพื่อตรวจสอบ และควบคุมผ่านการสื่อสารที่เชื่อถือได้ ดังนั้นจึงมีการให้ความสนใจในการศึกษาไมโครกริดเพิ่มขึ้น [7] แม้ว่าการพึ่งพากันกันระหว่างไมโครกริดจะมีความซับซ้อนก็ตาม

ในการศึกษานี้ได้ศึกษาโครงสร้าง และแนวคิดเกี่ยวกับความปลอดภัยทางไซเบอร์ของไมโครกริด เริ่มตั้งแต่การโจมตีที่มุ่งเป้าไปกับอุตสาหกรรม การรักษาความปลอดภัยทางไซเบอร์ด้านพลังงาน จุดอ่อนของระบบเครือข่าย การควบคุมไมโครกริดภายใต้การโจมตีทางไซเบอร์ การสื่อสารในไมโครกริด การวิเคราะห์ผลกระทบการโจมตีทางไซเบอร์ โครงสร้างการควบคุมที่ใช้ในไมโครกริด การควบคุมอัตโนมัติเพื่อป้องกันการโจมตีทางไซเบอร์ และส่วนสุดท้ายการทดสอบแบบการจำลองร่วม จากมุมมองที่แตกต่างกัน

วิธีการศึกษา

1. การโจมตีทางไซเบอร์ที่เกิดกับอุตสาหกรรม

ในศตวรรษที่ 21 ได้เริ่มเห็นเหตุการณ์ทางไซเบอร์ต่างๆ ที่ส่งผลกระทบต่อโครงสร้างพื้นฐาน ความซับซ้อนของการโจมตีทางไซเบอร์ในระบบควบคุมอุตสาหกรรม (Industrial Control Systems : ICS) เผยให้เห็นระดับความชำนาญของผู้โจมตีระบบควบคุม [8] การเชื่อมต่อโครงข่ายอินเทอร์เน็ตของไมโครกริดทำให้เกิดอันตรายในรูปแบบต่างๆ

Stuxnet เป็นมัลแวร์คอมพิวเตอร์ ที่ใช้ในการโจมตีระบบควบคุม และโปรแกรมควบคุมการทำงานอุตสาหกรรม (ICS) ซึ่งใช้ในระบบส่งน้ำในอุตสาหกรรม หรือระบบอื่นๆ ที่เกี่ยวข้องกับอุตสาหกรรม มัลแวร์นี้เป็นหนึ่งในการโจมตีทางไซเบอร์ที่มีความซับซ้อน และรุนแรงที่สุดที่เคยรู้จัก มีจุดประสงค์เพื่อทำลายหรือยับยั้งระบบ

ควบคุม และการควบคุมในโรงงานหรืออุตสาหกรรม โดยเฉพาะในกรณีของ Stuxnet เป็นการโจมตีที่เน้นยับยั้งการทำงานของโรงงานนิวเคลียร์ในอิหร่านในปี 2010 และถูกค้นพบว่ามีส่วนผู้บุกรุกสร้างมาอย่างมืออาชีพเพื่อทำลายระบบนั้นๆ โดยมีความเฉพาะเจาะจงสูง และใช้ช่องโหว่ความปลอดภัยที่เรียกว่า "zero-day" เพื่อเข้าถึงระบบ และเปลี่ยนแปลงค่าอุณหภูมิ และแรงดันที่สำคัญในโรงงานนิวเคลียร์ ทำให้เกิดความเสียหาย และเกิดความร้อนในการดำเนินงานของโรงงานนั้น [9] Duqu เป็นมัลแวร์ที่ถูกออกแบบมาเพื่อรวบรวมข้อมูลที่เป็นประโยชน์จากระบบเป้าหมาย โดยส่งข้อมูลนี้ไปยังผู้บุกรุก เป้าหมายหลักของ Duqu คือการจัดการข้อมูลที่สำคัญและการสร้างโปรไฟล์ผู้ใช้เพื่อใช้ในการโจมตีต่อไป โดยที่ไม่ทำลายระบบเป้าหมาย และ Flame เป็นมัลแวร์ที่ซับซ้อนมาก มีวัตถุประสงค์ในการแอบโจรกรรมทางไซเบอร์ การระบาดของมัลแวร์นี้เหมือนใยแมงมุม เพราะมีความสามารถในการจัดการข้อมูลที่รวบรวมได้ และการร่วมมือกับอื่น ๆ ในการคุกคามบนเครือข่าย ทั้ง Duqu และ Flame เป็นมัลแวร์ที่ซับซ้อนเพื่อการโจมตีทางไซเบอร์ที่มุ่งเน้นที่ระบบควบคุมอุตสาหกรรม แม้ว่าความสัมพันธ์ของมัลแวร์เหล่านี้กับ Stuxnet ยังไม่ชัดเจน แต่มัลแวร์เหล่านี้ได้รับความสนใจจากนักวิจัย และผู้เชี่ยวชาญด้านความปลอดภัยทาง-ไซเบอร์ในระดับโลกเนื่องจากความซับซ้อน และความเสี่ยงที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ในระดับอุตสาหกรรม [10] DoS (Denial of Service) Attack คือการโจมตีที่จัดทำขึ้นเพื่อทำให้บริการหรือแหล่งทรัพยากรต่างๆ ไม่สามารถให้บริการได้ตามปกติ โดยทำให้ระบบหรือเครื่องไม่สามารถรับหรือประมวลผลคำขอจากผู้ใช้ได้ เป้าหมายหลักของ DoS Attack คือการทำให้บริการไม่สามารถให้บริการแก่ผู้ใช้ที่ถูกต้อง ซึ่งอาจทำให้ผู้ใช้ไม่สามารถเข้าถึงบริการออนไลน์ที่ถูกโจมตีได้ การโจมตีประเภทนี้สามารถทำได้หลายวิธี เช่น การส่งคำขอมากมายไปยังเครื่องบริการเพื่อเกินความจุของระบบ การโจมตีด้วยการใช้ช่องโหว่ของระบบ หรือการทำให้เครื่องหรือเครือข่ายหยุดทำงานโดยการเน้นที่ทรัพยากรที่สำคัญ การป้องกัน DoS- Attack มักจะเน้นที่การใช้เทคโนโลยีและมาตรการความปลอดภัยที่เหมาะสม เช่น การใช้วิธีการกรองแพคเก็ตการตั้งค่า Firewalls และการตรวจจับการโจมตีที่เป็นไปได้

ในเดือนธันวาคม 2015 มีการโจมตีทางไซเบอร์ที่เกิดขึ้นในยูเครนทำให้มีการดับไฟฟ้าบริเวณกว้าง และกระทบลูกค้าประมาณ 225,000 ราย การโจมตีนี้เกี่ยวข้องกับโทรจัน รุ่นใหม่ที่ชื่อว่า Disakil ตามรายงานจากบริษัทพลังงาน สถาบัน SANS และ Electricity Information Sharing and the Analysis Center (E-ISAC) ปัญหาเริ่มต้นมาหลายเดือนก่อนการโจมตีจริง โดยการติดตั้งมัลแวร์ผ่านการโจมตีแบบฟิชชิ่งทางอีเมล ในระหว่างช่วงเวลานี้ แฮกเกอร์ได้ตรวจสอบ และเก็บรวบรวมข้อมูลที่มีค่าเกี่ยวกับการทำงานของระบบในระหว่างสิ่งที่เรียกว่าระยะการลาดตระเวน (reconnaissance) ในวันที่เกิดเหตุ ผู้โจมตีได้เข้าควบคุม Human Machine Interface (HMI) และตัดไฟฟ้าโดยเปิดเบรกเกอร์ตามจำนวนที่กำหนดเพื่อสกัดกั้นการกู้คืนบริการ โดยใช้การโจมตีแบบปฏิเสธการบริการ (DoS) บนเครือข่ายการสื่อสาร และปิดกั้นการรายงานปัญหาจากลูกค้าผ่านสายโทรศัพท์แบบคลาสสิก นอกจากนี้ มีการใช้มัลแวร์ที่สามารถจดจำซอฟต์แวร์ระบบได้เพื่อบล็อกแอปพลิเคชันที่กำหนดขอบเขตการหยุดทำงาน [11,12]

2. การรักษาความปลอดภัยทางไซเบอร์ด้านพลังงาน

สำนักงานพลังงานระหว่างประเทศ (IEA) ให้คำนิยามความมั่นคงด้านพลังงานว่าเป็น "แหล่งพลังงานที่มีอยู่อย่างต่อเนื่องในราคาที่เหมาะสม" ซึ่งการรักษาความปลอดภัยด้านพลังงานสามารถดำเนินการในระดับพื้นฐาน 2 ระดับ คือ

1. การรักษาความปลอดภัยระยะสั้น เน้นในเรื่องของเสถียรภาพของการจัดหาและการใช้งานอุปสงค์และอุปทานในระยะสั้น นั่นหมายถึงการให้ความสำคัญกับการให้พลังงานอย่างเหมาะสมและมีความเพียงพอในระยะเวลาสั้น ๆ เพื่อให้ระบบพลังงานสามารถทำงานได้ตลอดเวลาโดยไม่มีขาดขาด

2. การรักษาความปลอดภัยในระยะยาว เน้นไปที่การลงทุนและมาตรการที่สนับสนุนข้อกำหนดทางเศรษฐกิจและการพัฒนาที่ยั่งยืนในระยะยาว เช่น การพัฒนาแหล่งพลังงานทดแทนและความยืดหยุ่นในระบบพลังงานเพื่อให้ระบบสามารถปรับตัวให้รองรับการเปลี่ยนแปลงกะทันหันของโหลดกริด และเงื่อนไขสภาพแวดล้อม

ไมโครกริดมีแนวโน้มการใช้งานเพิ่มขึ้นจึงมีการกำหนดมาตรฐาน IEEE 2030-2011 โดยเป็นองค์ประกอบของโครงสร้างพื้นฐานที่ทำงานร่วมกันได้ 3 แบบ ดังภาพที่ 1 การพึ่งพาซึ่งกันทำให้ปัญหาด้านความปลอดภัยมีความซับซ้อนขึ้น ควบคู่ไปกับการสร้างวิธีการใหม่ และฉลาดขึ้นในการรักษาความปลอดภัยในไมโครกริด

ภาพที่ 1 โครงสร้างไมโครกริดที่ถูกออกแบบ และสร้างตามมาตรฐาน IEEE 2030

การประเมินความปลอดภัยที่ศึกษาในปัจจุบันมุ่งเน้นไปที่การระบุช่องโหว่ที่อาจเกิดขึ้นจากชั้นไซเบอร์และการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นกับระบบพลังงาน ซึ่งก่อให้เกิดขอบเขตการวิจัยใหม่ที่เรียกว่าความปลอดภัยทางไซเบอร์ เป็นการออกแบบทางวิศวกรรมร่วมกันระหว่างทางกายภาพ และการคำนวณ โดยความมั่นคงทางกายภาพจะทำงานในระบบพื้นฐานที่สำคัญ และความมั่นคงทางไซเบอร์ มีหน้าที่ในการเพิ่มการสำรวจและประมวลผล และยังมีการพัฒนาอุปกรณ์ และแอปพลิเคชัน [13] ขึ้นในระบบ หลักการความปลอดภัยที่สำคัญที่สุด คือ การสื่อสารและการโอนข้อมูลในระบบเครือข่ายเรียกว่า CIA-triad ประกอบด้วย

Confidentiality หมายถึงการรักษาข้อมูลให้เป็นความลับ และปกป้องไม่ให้ถูกเปิดเผยหรือเข้าถึงโดยบุคคลหรือองค์กรที่ไม่มีสิทธิ์ นั่นคือความมั่นใจในการรักษาความลับของข้อมูลที่ได้รับมอบหมาย สำคัญอย่างยิ่งในหลายสถานการณ์ เช่น ในธุรกิจ การแพทย์ และกลุ่มงานที่เกี่ยวกับข้อมูลที่มีความลับ การละเมิดอาจทำให้เกิดผลกระทบที่รุนแรงต่อองค์กรหรือบุคคลที่เกี่ยวข้อง

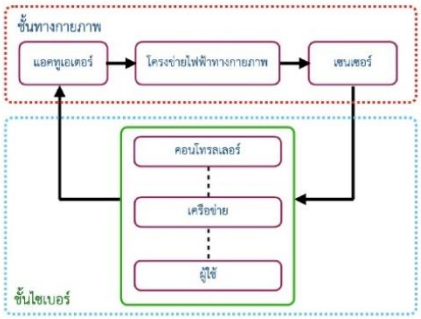
Integrity หมายถึงความซื่อสัตย์และความเป็นธรรมของบุคคลหรือองค์กร การทำตามมาตรฐานทางวินัยทางจริยธรรม และความสมบูรณ์ทางจริยธรรม เน้นการป้องกันการเปลี่ยนแปลงหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตขณะที่ข้อมูลถูกโอนหรือเก็บรักษา เพื่อรักษาความถูกต้องของข้อมูล

Availability หมายถึงความพร้อมให้บริการหรือทราบในทุกขณะที่มีความต้องการ ซึ่งส่วนนี้เป็นส่วนสำคัญของความมั่นคงปลอดภัยของข้อมูลและระบบ ในบริบทของเทคโนโลยีและระบบสารสนเทศ availability นั่นคือความสามารถให้บริการหรือให้ใช้ข้อมูลหรือทรัพยากรต่างๆ ได้ตลอดเวลา เป็นสิ่งสำคัญเพราะหากมีปัญหาเกี่ยวกับความพร้อมให้บริการ องค์กรหรือระบบอาจประสบกับปัญหาในการดำเนินกิจกรรมปรกติ สูญเสียข้อมูล หรือมีผลกระทบต่อการทำงานของระบบ มักถูกนำเสนอในรูปแบบของระยะเวลาที่ระบบพร้อมให้บริการ และระยะเวลาที่ระบบไม่สามารถให้บริการได้

หลักการเหล่านี้เป็นพื้นฐานสำคัญของความปลอดภัยข้อมูลในระบบเครือข่าย IT เป็นสิ่งสำคัญในการป้องกันข้อมูล เพื่อให้การทำงานของระบบและการสื่อสารเป็นปกติ ความมั่นคงของไมโครกริดถูกสร้างขึ้นโดยใช้หลักการเดียวกันกับที่กล่าวมาข้างต้น แต่มีความแตกต่างในลำดับความสำคัญ โดยให้ความสำคัญกับความพร้อม

การใช้งานมากที่สุด รองลงมาคือประสิทธิภาพ ความรับผิดชอบ และความลับของข้อมูล โดยมีการอ้างถึงความรับผิดชอบเป็นเกณฑ์ความมั่นคงเพิ่มเติมด้วย [14] ระบบการป้องกัน ที่ควบคุมความปลอดภัยใช้เทคโนโลยีอิเล็กทรอนิกส์เพื่อป้องกัน และควบคุมการเข้าถึงไม่พึงประสงค์หรือไม่มีสิทธิ์เข้าถึงในพื้นที่หรือระบบที่มีความลับหรือสำคัญหรือที่เรียกว่า Electronic Security Perimeter (ESP) ส่วนใหญ่เน้นการใช้เทคโนโลยีอิเล็กทรอนิกส์ เช่น firewall intrusion detection systems virtual private-networks (VPN) และการใช้ encryption เพื่อปกป้องข้อมูลและระบบต่าง ๆ ที่เชื่อมต่อกับโครงสร้างนั้น มีไวรัส การบุกรุก หรือการเข้าถึงที่ไม่พึงประสงค์เป็นต้นคือภัยคุกคามที่ ESP จะต้องป้องกัน การสร้าง ESP เป็นส่วนสำคัญในการดูแลความปลอดภัยของระบบและข้อมูลในโลกดิจิทัล

การโจมตีทางไซเบอร์ต่อระบบกายภาพ (Cyber-Physical Systems : CPS_s) มีความหลากหลายซึ่งอาจถูกเรียกชื่อในมุมมองที่แตกต่างกัน เช่น Bias Injection Zero Dynamics DoS การโจมตีแบบตักฟัง การโจมตีแบบซ้ำ การโจมตีแบบซ่อนเร้น การโจมตีแบบแอบแฝง และการโจมตีการส่งข้อมูลเท็จไดนามิก [16] แต่การโจมตีเหล่านี้สามารถป้องกันได้โดยทำได้ตามเกณฑ์ความปลอดภัยตามรูปแบบของการโจมตีทางไซเบอร์ที่แสดงในภาพที่ 2 ตามต้องการความรักษาความปลอดภัยของระบบ การจัดประเภทการโจมตีดังกล่าวจะขึ้นอยู่กับผลกระทบที่มีต่อเกณฑ์ความปลอดภัยนี้ ซึ่งจะช่วยในการเข้าใจ และจัดการกับการโจมตีทางไซเบอร์อย่างเหมาะสม [16]



ภาพที่ 2 รูปแบบของการโจมตีทางไซเบอร์

การศึกษานี้เน้นการโจมตีทางไซเบอร์ที่เกิดขึ้นอย่างร้ายแรง ซึ่งไม่เพียงแค่มีผลกระทบทางด้านเทคนิคเท่านั้น แต่ยังมีผลกระทบทางเศรษฐกิจ และมีผลกระทบเป็นวงกว้างในระบบไฟฟ้า รูปแบบการโจมตีเริ่มต้นจากการแก้ไขข้อมูลเครื่องวัด หรือควบคุมการใช้งานโหลดในอนาคต และสร้างความเสียหายกับอุปกรณ์ หรือเกิดไฟฟ้าดับเป็นวงกว้าง [17] วิธีการดังกล่าวนั้นมีความซับซ้อน เพราะต้องพิจารณาข้อกำหนดทางกายภาพของระบบและสถานะของระบบไฟฟ้าที่มีการป้องกันแบบร่วมสมัย ผู้โจมตีจึงต้องมีความรู้ และความเข้าใจเกี่ยวกับลักษณะทางกายภาพของระบบ และสมรรถนะของคอมพิวเตอร์ ซึ่งจะเป็นอุปกรณ์ที่จำเป็นในการโจมตี [18] อย่างไรก็ตามกลยุทธ์ที่มีประสิทธิภาพในการป้องกันเหตุการณ์ดังกล่าวมีส่วนสำคัญ 2 ส่วน คือ

1. การพัฒนามาตรการตรวจจับ และจัดการ เป็นการพัฒนามาตรการที่สามารถตรวจจับการโจมตีที่เป็นอันตราย และจัดการกับสาเหตุของการติดไวรัสในระบบ เป็นส่วนสำคัญของกลยุทธ์อาจรวมถึงการตรวจสอบรายการกิจกรรมในเครือข่ายเพื่อระบุแนวโน้มของการโจมตี หากพบความผิดปกติหรือการรุกเข้ามา ก็จะทำการแยกสาเหตุของการโจมตี นอกจากนี้ยังมีมาตรการป้องกัน และตอบสนองที่เข้มงวดเพื่อป้องกันไม่ให้ฝ่ายตรงข้ามเข้าถึงระบบได้

2. ความสามารถในการฟื้นตัวทางไซเบอร์ เป็นการวางแผน และเตรียมความพร้อมที่ระบบไซเบอร์จะได้รับการโจมตี และอธิบายรายละเอียดเกี่ยวกับวิธีการกู้คืนจากการโจมตีเหล่านี้ให้มีอย่างรวดเร็วเป็นส่วนสำคัญของวิธีการนี้ ซึ่งจะช่วยให้ระบบสามารถกู้คืน และทำงานอย่างปกติใหม่โดยรวดเร็วในกรณีเหตุการณ์ไม่คาดคิดทางไซเบอร์

ความแตกต่างระหว่างการรักษาระบบให้ปลอดภัย และความเรียบง่ายในการเข้าใจการทำงานของระบบเป็นปัญหาที่สำคัญในการออกแบบ และดำเนินการในระบบพลังงานแบบอัจฉริยะ การทำให้ระบบปลอดภัยอาจต้องใช้มาตรการความปลอดภัยที่ซับซ้อนเพื่อป้องกันการโจมตีทางไซเบอร์ ทำให้ระบบมีความซับซ้อนเพิ่มขึ้น แต่ในระยะยาว การทำให้ระบบมีความเรียบง่ายในการเข้าใจและดำเนินการนั้นเป็นสิ่งที่สำคัญเพื่อให้ผู้ใช้สามารถรับรู้และปรับตัวต่อการทำงานของระบบได้อย่างถูกต้อง และมีประสิทธิภาพ ดังนั้นการออกแบบความปลอดภัยควรพิจารณาความเรียบง่ายในการดำเนินการ และการเข้าใจระบบเช่นกัน โดยปรับสมดุลเพื่อให้ได้ผลลัพธ์ที่เหมาะสมและคุ้มค่าสำหรับการดำเนินการในระบบพลังงานอัจฉริยะในระยะยาว การคำนึงถึงหลักการทั้งสองนี้เป็นสิ่งสำคัญในด้านความปลอดภัยที่มีประสิทธิภาพในระบบพลังงานแบบอัจฉริยะ

3. จุดอ่อนของระบบเครือข่าย

ระบบจำหน่ายไฟฟ้า และการเชื่อมโยงระหว่างการผลิตกับการใช้พลังงานไฟฟ้าของผู้บริโภค มีบทบาทสำคัญในการส่งพลังงานไฟฟ้าจากแหล่งผลิตไปยังผู้ใช้งาน ระบบนี้มักถูกออกแบบเพื่อให้การส่งพลังงานเป็นไปในทิศทางเดียว ผู้ที่ดูแลระบบต้องรับมือกับการเปลี่ยนแปลงที่สำคัญในระบบไฟฟ้า โดยเฉพาะในระดับแรงดันไฟฟ้าที่ระหว่างระดับปานกลางถึงระดับต่ำ ความเปลี่ยนแปลงของพลังงานในระบบเกิดจากหลายปัจจัย เช่น การเพิ่มการใช้พลังงานไฟฟ้าจากแหล่งพลังงานหมุนเวียน การใช้เทคโนโลยีใหม่ ๆ ที่เชื่อมโยงกับระบบไฟฟ้า เช่น ระบบจำหน่ายไฟฟ้าอัจฉริยะ หรือการเปลี่ยนแปลงในการใช้พลังงานไฟฟ้าโดยผู้บริโภค ผู้ดำเนินการระบบจำหน่ายจะต้องรักษาเสถียรภาพ และวางแผนเพื่อให้ระบบไฟฟ้ายังคงทำงานได้อย่างมีประสิทธิภาพ และปลอดภัยในสถานการณ์ที่มีการเปลี่ยนแปลงนี้ นี่คือปัจจัยสำคัญในการพัฒนาระบบพลังงานแบบอัจฉริยะที่สามารถทำงานอย่างมีประสิทธิภาพ และมีความยืดหยุ่นในการดำเนินงานในสถานการณ์ที่เปลี่ยนแปลงได้ [6]

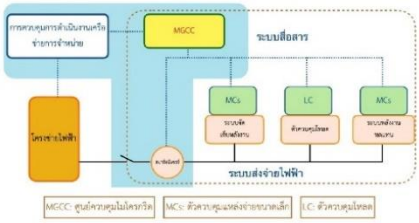
การประยุกต์ใช้ระบบการจัดการพลังงาน (Energy Management System : EMS) ในระบบส่งไฟฟ้า และการประยุกต์ใช้ EMS ในระดับการจำหน่ายไฟฟ้ามีความแตกต่างกัน ในระบบส่งไฟฟ้าถูกใช้ในช่วงต้นทศวรรษ 1970 เพื่อจัดการ และควบคุมการผลิตพลังงานไฟฟ้าในระบบส่งไฟฟ้า โดยเน้นการควบคุมกระบวนการผลิตไฟฟ้าให้ทำงานอย่างมีประสิทธิภาพ และปลอดภัยในเวลาเดียวกัน มักใช้เทคโนโลยี และแนวทางด้านวิศวกรรมเพื่อปรับปรุงประสิทธิภาพของระบบส่งไฟฟ้า ในทางกลับกันการประยุกต์ใช้ EMS ในระดับการจำหน่ายไฟฟ้าไม่ได้มีการใช้บ่อย เป็นเพราะระบบการจัดการพลังงานในระดับการจำหน่ายมีความซับซ้อนที่แตกต่างจากระบบส่งไฟฟ้า การจัดการพลังงานในระดับการจำหน่ายเน้นการจัดส่งพลังงานไฟฟ้าจากหลายแหล่งผลิตไปยังผู้ใช้งาน และมีการควบคุม จัดการกับการจำหน่าย และการใช้พลังงานไฟฟ้าของผู้บริโภค [19] เป็นการใช้เทคโนโลยีเพื่อรวมทรัพยากรพลังงานจากแหล่งต่าง ๆ และการให้บริการพลังงานแก่ผู้ใช้ในลักษณะที่ยืดหยุ่น และมีประสิทธิภาพ เช่น การใช้พลังงานแสงอาทิตย์ และพลังงานลมจากแหล่งในพื้นที่ใกล้เคียงผู้ใช้งาน นอกจากนี้เทคโนโลยีที่เกี่ยวข้องกับการจัดการพลังงานแบบสมาร์ท และการตอบสนองความต้องการของผู้ใช้ที่มีประสิทธิภาพมากขึ้นกำลังเป็นที่นิยมในปัจจุบัน ทั้งนี้การนำเทคโนโลยีมาใช้ในการแก้ปัญหาด้านพลังงาน และการจัดการทรัพยากรที่กระจายตัวได้ทั้งหมดเป็นแนวโน้มที่มีการวิจัย และพัฒนาอย่างต่อเนื่องเพื่อสร้างสิ่งจูงใจในการสร้างโซลูชันที่ยั่งยืน มีประสิทธิภาพสำหรับการจัดการพลังงานในอนาคต [5]

ความยืดหยุ่นในการผลิตไฟฟ้า และจัดส่งในระบบไฟฟ้าแบบกระจาย โดยส่วนใหญ่จะเป็นแหล่งพลังงานที่ใช้งานแบบที่สามารถควบคุมการเปิด และปิดเพื่อตรงกับความต้องการของเครือข่ายไฟฟ้าในเวลาที่ต่างกัน โดยเฉพาะในช่วงที่มีความต้องการสูงหรือข้อมูลจากระบบ EMS หรือระบบควบคุมไฟฟ้าส่วนกลางแสดงว่ามีความต้องการเพิ่มการผลิตไฟฟ้าเพิ่มขึ้น การใช้ Distributed Generation (DG) นี้เป็นทางเลือกที่มีประโยชน์ในช่วงที่มีความต้องการพลังงานสูง และช่วยลดความเครียดในระบบไฟฟ้า แต่อย่างไรก็ตามการจัดการ และควบคุมการใช้ DG ให้มีประสิทธิภาพเป็นสิ่งสำคัญเพื่อป้องกันปัญหาที่อาจเกิดขึ้นในระบบไฟฟ้ารวมถึงให้ความยืดหยุ่นประสิทธิภาพในการผลิต และส่งพลังงานไฟฟ้าให้ตรงกับความต้องการของผู้ใช้งานได้อย่างมีประสิทธิภาพ [19]

4. การควบคุมไมโครกริดภายใต้การโจมตีทางไซเบอร์

เพื่ออธิบายแนวคิดของไมโครกริด [20,21] เชื่อว่าไมโครกริดเป็นทางออกที่ดีที่สุดสำหรับการบูรณาการและการควบคุมที่เชื่อถือได้ของระบบพลังงานแบบกระจาย (Distributed Energy Resources : DER) รวมถึงระบบกักเก็บพลังงาน (Energy Storage System : ESS) และโหลดที่ควบคุมได้ [22] ในทำนองเดียวกัน [23,24] ไมโครกริดถูกมองว่าเป็นเรื่องที่น่าสนใจในการบูรณาการพลังงานหมุนเวียนที่มีอยู่จำนวนมาก แต่ยังคงไม่ได้นำมาใช้งานกันอย่างแพร่หลายเนื่องจากความไม่ยืดหยุ่นของเครือข่ายในปัจจุบัน นอกจากนี้ DER แต่ละตัวมักจะมีขนาดเล็กเกินไปซึ่งเป็นอีกหนึ่งปัญหาที่ต้องได้รับการแก้ไข

โครงสร้างของไมโครกริด มีความพยายามในการกำหนดค่าที่เป็นมาตรฐานของ Block Diagram ซึ่งยังไม่ประสบผลสำเร็จ [13,23] สิ่งสำคัญ คือ ต้องสังเกตว่าไมโครกริดสามารถปรับให้เข้ากับข้อกำหนดค่าต่าง ๆ และการปรับตามฟังก์ชันของข้อกำหนด ดังภาพที่ 3 แสดงโครงสร้างทั่วไปสำหรับไมโครกริดสมัยใหม่ ไมโครกริดที่เชื่อมต่อกับระบบไฟฟ้าสร้างขึ้นเพื่อทำงานในโหมดเชื่อมต่อแบบอิสระ หรือโหมดเชื่อมต่อกับระบบไฟฟ้า อาจมีจุดเชื่อมต่อหนึ่งจุดหรือหลายจุด [8] ไมโครกริดแบบ stand-alone จะไม่มีจุดเชื่อมต่อร่วม (Point of Common Coupling : PCC) กับกริดหลัก [17]



ภาพที่ 3 โครงสร้างทั่วไปสำหรับไมโครกริดสมัยใหม่

ประสิทธิภาพในการทำงานของไมโครกริดจำเป็นต้องมีการวัด การสื่อสาร และการควบคุมที่มีประสิทธิภาพ ซึ่งข้อมูลที่ได้ต้องอาศัยเครื่องมือวัดประเภท เซ็นเซอร์ แอคชูเอเตอร์ และอุปกรณ์ภาคสนามต่างๆ [16] ไมโครกริดเป็นระบบที่มีความไวสูง [13] ซึ่งในทางกายภาพจะได้รับผลกระทบอย่างมากเมื่อเครือข่ายของระบบไม่สมบูรณ์ เนื่องจากไม่มีการตรวจจับความปลอดภัย ด้วยเหตุนี้ผู้โจมตีจึงมีโอกาสมากขึ้นที่จะก่อกวนให้เกิดปัญหาร้ายแรงในไมโครกริด ซึ่งนำไปสู่ความเสียหายจากการโจมตี [25] การรักษาความปลอดภัยของไมโครกริดในการโจมตีทางไซเบอร์ต่อระบบไฟฟ้ามักจะถือว่าการโจมตีเหล่านี้เป็นสัญญาณรบกวน ดังนั้นจึงมีความพยายามที่กำจัดการรบกวนเหล่านี้โดยใช้เทคนิคการกรอง [26,27] อย่างไรก็ตาม เทคนิคเหล่านี้ขึ้นอยู่กับสถิติ ซึ่งจะสูญเสียประสิทธิภาพเมื่อเผชิญกับการโจมตีที่มีการปรับแต่งเพิ่มเติม [11]

5. การสื่อสารในไมโครกริด

เครือข่ายการสื่อสารของไมโครกริดถือเป็นสิ่งสำคัญที่ส่งผลให้มีประสิทธิภาพ การควบคุมระบบแบบกระจาย และแบบอิสระ สถานะของเครือข่าย ปัญหาการสื่อสารในไมโครกริด มักมาจากเทคโนโลยีการสื่อสารที่ต่างประเภทกัน [13] การสื่อสารบนอินเทอร์เน็ตมีการใช้งานเพิ่มขึ้น ซึ่งเสี่ยงต่อการถูกโจมตีทางไซเบอร์มากแต่ก็ยังจำเป็นที่ยังต้องใช้เครือข่ายเพื่อเชื่อมต่ออุปกรณ์เครื่องมือวัดในไมโครกริด เช่น ข้อมูลพยากรณ์อากาศ ราคาเชื้อเพลิง ชั่วโมงเร่งด่วน [13]

ในอีกด้านหนึ่งการตรวจจับการบุกรุก ไฟร์วอลล์ พื้นฐานในการรักษาความปลอดภัยแบบดั้งเดิมสามารถประยุกต์ใช้ในการป้องกันการโจมตีทางไซเบอร์ในไมโครกริดได้ [28] มีจำลองเครือข่ายการสื่อสารที่ถูกโจมตีของระบบไฟฟ้า และพยายามทำการจำลองการโจมตีเป็นการหน่วงเวลาภายในรอบการควบคุม [29] การตรวจสอบความล่าช้าในการสื่อสาร ซึ่งอาจเกิดปัญหาความไม่เสถียรของระบบ ได้มีการนำเสนอแนวทางการควบคุมโดยใช้สัดส่วน–ปริพันธ์ (PI) ที่จะควบคุมความถี่ ซึ่งสามารถใช้ได้ในไมโครกริด

อย่างไรก็ตาม สมมติฐานลักษณะของผลกระทบจากการโจมตีนั้นมีความเรียบง่ายเกินไป [30,31] ไมโครกริดยังมีอัตราความล่าช้าระหว่างแหล่งที่มาทำให้เกิดความล่าช้าของเครือข่าย [32] การนำปัญหาการสื่อสารไปสู่ขอบเขตที่ใหญ่ขึ้น Cyber–Physical Power System (CPPS) [33] สิ่งที่เป็นการกำหนดค่าการสื่อสารที่ดีกว่าในแง่ของการป้องกันความล้มเหลวแบบเรียงซ้อน ในการเปรียบเทียบ โดยขึ้นอยู่กับค่าขีดจำกัดประสิทธิภาพการส่งข้อมูล พวกเขาพบว่าเครือข่ายการสื่อสารแบบ Double–Star ทำงานได้ดีกว่าเครือข่ายการสื่อสารแบบ Networks

การป้องกันความล้มเหลวแบบเรียงซ้อนใน CPPS เป็นเรื่องที่มีความสำคัญในการควบคุม และความปลอดภัยของระบบพลังงานที่เชื่อมต่อกันผ่านเครือข่าย การวิเคราะห์กลไก และลักษณะไดนามิกที่ครอบคลุมของเครือข่ายที่พึ่งพาซึ่งกันและกัน ความสัมพันธ์การเชื่อมต่อระหว่างระบบไฟฟ้า และระบบสื่อสารมีความสำคัญในการป้องกันการล้มเหลวแบบเรียงซ้อน การเสนอแบบจำลองที่พึ่งพาซึ่งกันและกันแบบใหม่ด้วยรูปแบบการเชื่อมโยงแบบ "มุมทางไฟฟ้า" พบว่าแบบจำลองนี้มีประสิทธิภาพในการลดความน่าจะเป็นของเหตุการณ์ไฟดับเป็นวงกว้างที่เกิดจากการโจมตีแบบสุ่ม และในกรณีของการโจมตีที่เป็นอันตราย เอาต์พุตการจำลองเชื่อมต่อระบบไฟฟ้า และการสื่อสารแสดงถึงความสำคัญของความแข็งแกร่งของการเชื่อมต่อระหว่าง ระบบไฟฟ้ามากกว่าการเลือกแบบจำลองที่พึ่งพาซึ่งกันและกัน เนื่องจากระบบไฟฟ้าที่เชื่อมต่อกับระบบสื่อสารมีความเสี่ยงมากกว่าในกรณีที่ระบบสื่อสารน้อยลง การป้องกันความล้มเหลวในระบบไฟฟ้าทางกายภาพเป็นสิ่งสำคัญเพื่อความปลอดภัยและเสถียรของระบบไฟฟ้านี้

ภาพที่ 4 แสดงกลไก และแนวทางในการต่อต้านการแทรกแซงทางไซเบอร์ในโดเมนการสื่อสาร

ใน [34] การวิเคราะห์ช่องโหว่ได้เจาะลึกลงไปในโครงสร้างเฟรมเวิร์ก IEEE C37.118 ไปยังส่วนประกอบที่อ่อนแอที่สุด ซึ่งก็คือชั้นโปรโตคอลการสื่อสาร ในขณะที่วิเคราะห์ความอ่อนไหวของสองโปรโตคอลที่ใช้กันทั่วไปในชั้นการสื่อสาร เช่น Transmission control Protocol (TCP) และ User Datagram Protocol (UDP) ต่อการโจมตี DoS และ FDI จึงได้สรุปข้อกำหนดที่จะใช้ในการสร้างการบุกรุกทางไซเบอร์ตลอดจนการป้องกัน ดังภาพที่ 4 แสดงสรุปแนวทางที่นำเสนอซึ่งอธิบายกลไก และแนวทางที่พิจารณาในการต่อต้านการแทรกแซงทางไซเบอร์ในการสื่อสาร

6. การวิเคราะห์ผลกระทบการโจมตีทางไซเบอร์

การพิสูจน์ว่าขั้นตอนทางกายภาพ และทางไซเบอร์สำหรับระบบไฟฟ้าไม่ได้เป็นเพียงการแก้ปัญหาที่จะเกิดปัญหาเท่านั้น แต่ยังมีความพยายามในด้านการประเมินผลกระทบ และการสร้างแบบจำลองภัยคุกคามเพื่อลดความเสี่ยงไม่ให้เกิดการโจมตีทางไซเบอร์ที่ทำให้เกิดเหตุการณ์จริง และความเสียหายทางกายภาพได้ดีขึ้น

ความเป็นไปได้ที่จะมีการโจมตีจริง ๆ ที่เกิดขึ้นจากการโจมตีทางไซเบอร์ มีสองประเภทหลัก คือ การโจมตีความพร้อมใช้งาน และการโจมตีความถูกต้อง การโจมตีเหล่านี้เป็นอันตรายต่อระบบสารสนเทศ และระบบ Global Positioning System (GPS) ซึ่งเป็นส่วนสำคัญของการทำงานของไมโครกริดในโหมดที่แตกต่างกัน เช่น โหมดการเชื่อมต่อ โหมดอิสระ และโหมดการเชื่อมต่อระหว่างไมโครกริด [18]

7. โครงสร้างการควบคุมที่ใช้ในไมโครกริด

ระบบควบคุมของไมโครกริดมีความแตกต่างกันไปตามวัตถุประสงค์ในการใช้งาน โครงสร้างของการควบคุมสามารถปรับแต่งตามความต้องการ และข้อจำกัดในการใช้งาน เช่น ในโหมดเชื่อมต่อกับกริด ความถี่ และแรงดันไฟฟ้าถูกควบคุมโดยระบบไฟฟ้าหลักที่จุดเชื่อมต่อร่วม PCC การจัดการพลังงาน และการแบ่งโหลด การเปลี่ยนโหมดการทำงานระหว่างการเชื่อมต่อกับอิสระยังคงเป็นประเด็นสำคัญในระบบควบคุมของไมโครกริด โดยระบบควบคุมในพื้นที่รับผิดชอบสำหรับการควบคุมเสถียรภาพทั้งหมด โครงสร้างของการควบคุมนี้ยังจะแตกต่างกันขึ้นอยู่กับประเภทของไมโครกริด

อย่างไรก็ตามในทางปฏิบัติเราสามารถสรุปได้ว่ากลยุทธ์การควบคุมหลัก และรองมีความสัมพันธ์ที่สำคัญกับความเสถียรในการทำงานของไมโครกริด นอกจากนี้ความสอดคล้องระหว่างส่วนประกอบต่างๆ ก็มีบทบาทสำคัญในการควบคุม และประสานกันระหว่างไมโครกริด และระบบไฟฟ้าหลัก การประสานกันนี้มักถูกนำไปใช้โดยการควบคุมระดับสูงเพื่อให้ระบบทำงานอย่างมีประสิทธิภาพ และมีเสถียรภาพ [23] เดิมการควบคุมแบบกระจายเป็นวิธีการเพิ่มความสามารถในการปรับขนาด โดยจะแยกงานควบคุมระหว่างหน่วยต่างๆ แทนที่เพิ่มความสามารถในการคำนวณที่มากเกินไปเพียงอย่างเดียว นอกจากนี้ ความกระจัดกระจายของเครือข่ายการที่ใช้ในแผนการควบคุมแบบกระจายช่วยลดต้นทุนโครงสร้างพื้นฐาน [35] ไมโครกริดมีฟังก์ชันที่ฝังอยู่ในตัวควบคุมส่วนกลาง ซึ่งจะทำให้เกิดการประยุกต์ใช้ EMS ได้อย่างเหมาะสมที่สุด รวมถึงประสิทธิภาพเชิงเศรษฐกิจไปพร้อมๆ กับความพึงพอใจในข้อจำกัดในการปฏิบัติงานแบบเรียลไทม์

การเพิ่มประสิทธิภาพแบบกระจายได้รับแรงบันดาลใจจากปรากฏการณ์ทางชีววิทยา ระบบถูกออกแบบโดยใช้หลักการสื่อสารแบบเพียร์ทูเพียร์ ทำให้โมเดลนี้มีความยืดหยุ่น การควบคุมมีความเป็นได้อย่างมากในการควบคุมเสถียรภาพของการปรับสมดุลแรงดัน และความถี่

8. การควบคุมอัตโนมัติเพื่อป้องกันการโจมตีทางไซเบอร์

ระบบควบคุมในไมโครกริดเป็นระบบที่มีความเสี่ยงต่อการโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงการโจมตีด้วยการปฏิเสธบริการ และการโจมตีแบบการยับยั้งข้อมูล การโจมตีแบบธรรมดาสามารถตรวจจับ และ

ป้องกันได้ ผู้ป้องกันสามารถใช้วิธีการในการตรวจจับ และแยกแยะความผิดพลาดในระบบควบคุมหรือนำมาตรการป้องกันเบื้องต้นโดยการวางแผนความเสี่ยง และการวิเคราะห์ความมั่นคงปลอดภัย

การประเมินสถานะแบบคงที่ (Static State Estimator : SSE) นั้นมักถูกใช้ในการตรวจจับข้อมูลการวัดที่ไม่ถูกต้องในระบบส่งพลังงาน แต่ระบบนี้ก็ยังไม่ปลอดจากการโจมตี [37,38] การประเมินสถานะแบบเคลื่อนไหว (Dynamic State Estimation: DSE) เป็นสิ่งสำคัญสำหรับควบคุมไมโครกริดโดยเฉพาะอย่างยิ่งเมื่อมีจำนวน DER และการปรับปรุงระบบเพิ่มขึ้น วิธีการประเมินสถานะแบบกระจาย เช่น ตัวคาดการณ์ข้อมูลอินพุตที่ไม่รู้ (Unknown Input Observer : UIO) สามารถใช้ในการตรวจจับการโจมตี FDI ในไมโครกริด [36] การเพิ่มปัจจัยความเสี่ยงร่วมกัน (Cooperative Vulnerability Factor : CVF) ในตัวควบคุมความถี่ทางไฟฟ้าเพื่อเพิ่มความสามารถในการตรวจจับการโจมตีในไมโครกริด

ปัจจัยการป้องกันทางไซเบอร์ที่ใช้จะไม่เปลี่ยนแปลงในชั้นควบคุมกรรมวิธี (Secondary Distributed Control Layer) สามารถใช้ในการสร้างวิธีการตรวจจับที่สามารถตรวจจับการโจมตี FDI ในไมโครกริด [39] ประสิทธิภาพของการตรวจจับ และการป้องกันการโจมตีทางไซเบอร์ในไมโครกริดสามารถพัฒนาโดยการนำเอาความรู้ทางปฏิบัติ และเทคโนโลยีทางไซเบอร์ล่าสุดมาใช้ในการป้องกันความเสี่ยง เพื่อเพิ่มความปลอดภัยให้กับระบบพลังงานให้มากที่สุด

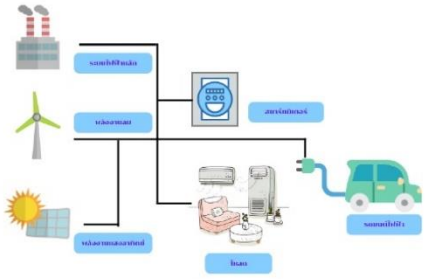
9. การทดสอบแบบการจำลองร่วม

การจำลองแบบ real-time เป็นวิธีที่มีความคุ้มค่าทางค่าใช้จ่ายสูงสุดสำหรับการศึกษาการทดลองในไมโครกริด การจำลองระบบพลังงานที่มีอุปกรณ์การสลับสับเปลี่ยนแหล่งจ่ายที่มีความเร็วสูง การแทนองค์ประกอบทางไซเบอร์ด้านกายภาพมีความยากลำบาก เนื่องจากความแตกต่างของระบบพลังงาน และระบบสื่อสาร การเชื่อมต่อซอฟต์แวร์จำลองแยกกันเพื่อรวมคุณสมบัติของทั้งสองระบบต้องมีการประสานงานและการแลกเปลี่ยนข้อมูล การเข้าใจเกี่ยวกับการทดลองที่มีอยู่ ข้อได้เปรียบ และข้อจำกัดของทดลองเป็นสิ่งสำคัญสำหรับการสร้างแบบจำลองการทดลองใหม่ การจำลองร่วม (Co-simulation) เป็นการสานต่อการทำงานของส่วนหนึ่งในการปฏิสัมพันธ์ในไมโครกริด ไม่ว่าจะผ่านเครื่องมือที่ระบุไว้เฉพาะหรือ platform-based [40]

10. สมาร์ทมิเตอร์ และความมั่นคงของข้อมูล

สมาร์ทมิเตอร์ และความมั่นคงของข้อมูล เป็นเรื่องที่สำคัญในระบบพลังงาน และไมโครกริด ดังนั้นจึงมีความจำเป็นที่จะศึกษาระบบความมั่นคงของข้อมูลที่เข้มงวดเพื่อปกป้องข้อมูล และความเป็นส่วนตัวของผู้ใช้พลังงานไฟฟ้า สมาร์ทมิเตอร์เป็นอุปกรณ์ที่ติดตั้งในบ้านหรือองค์กรของผู้ใช้ไฟฟ้าเพื่อวัด และตรวจสอบการใช้พลังงานไฟฟ้าได้โดยอัตโนมัติ สามารถส่งข้อมูลการใช้พลังงานไฟฟ้ากลับไปยังบริษัทพลังงานหรือผู้ให้บริการไฟฟ้าเพื่อให้ข้อมูลเกี่ยวกับการใช้พลังงานแก่ผู้ใช้และให้การควบคุมพลังงานได้มากขึ้น

ความมั่นคงของข้อมูลเกี่ยวกับสมาร์ทมิเตอร์เป็นสิ่งสำคัญ เนื่องจากข้อมูลเหล่านี้มีความสำคัญและเป็นความลับ เช่น ข้อมูลการใช้พลังงานของผู้ใช้ เรื่องแบบสอบถามส่วนบุคคล และข้อมูลการใช้พลังงานในช่วงเวลาที่แตกต่างกัน เมื่อมีการส่งข้อมูลจากสมาร์ทมิเตอร์ไปยังบริษัทพลังงาน หรือผู้ให้บริการไฟฟ้า ความมั่นคงของข้อมูลต้องรับการควบคุมอย่างเข้มงวดเพื่อป้องกันไม่ให้ข้อมูลสำคัญถูกชโมยหรือถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต การควบคุมความมั่นคงของข้อมูลของสมาร์ทมิเตอร์ประกอบด้วยมาตรการต่างๆ เช่น การเข้ารหัสข้อมูล การใช้ระบบความปลอดภัยทางสัญญาณ และการควบคุมการเข้าถึงข้อมูลด้วยสิทธิ์ และการรับรองตัวตน นอกจากนี้การกำหนดกฎ และข้อบังคับที่เกี่ยวข้องกับความมั่นคงของข้อมูลในสมาร์ทมิเตอร์มีความสำคัญ เพื่อให้ผู้ใช้ได้รับความคุ้มครองและมั่นใจในการใช้งานระบบสมาร์ท



ภาพที่ 5 รูปแบบการใช้งานสมาร์ทมิเตอร์

สมาร์ทมิเตอร์ได้รับการพัฒนามาจากการให้ข้อมูลการใช้ไฟฟ้าเบื้องต้นไปสู่การรองรับแอปพลิเคชันหลายรูปแบบ กลุ่มอุตสาหกรรมสมาร์ทมิเตอร์ของยุโรปได้กำหนดคุณสมบัติขั้นต่ำที่จำเป็นสำหรับสมาร์ทมิเตอร์ รวมถึงการอ่านระยะไกล และการสื่อสารสองทิศทาง สมาร์ทมิเตอร์สามารถสื่อสารการวัดแบบเรียลไทม์ที่สะสมข้อมูลและศูนย์ควบคุม ทำให้สามารถใช้งานฟังก์ชันการตอบสนองต่อความต้องการ และการพยากรณ์โหลดได้

โหมดการติดตั้ง และใช้งานขั้นสูงของการวัดสามารถให้ทราบค่าความสิ้นเปลืองพร้อมกับค่าใช้จ่าย และการเชื่อมต่อระบบสื่อสาร [41] การเลือกฟังก์ชันให้กับสมาร์ทมิเตอร์มีผลต่อระบบไฟฟ้า โดยมีข้อคำนึงเกี่ยวกับความลับของข้อมูล และการแก้ไขข้อมูล ดังภาพที่ 5

เทคโนโลยีบล็อกเชนสามารถแก้ไขปัญหาที่เกี่ยวข้องกับความมั่นคงของข้อมูลในสมาร์ทมิเตอร์และโครงสร้างพื้นฐานการวัดขั้นสูง [42] บล็อกเชนเป็นวิธีการเก็บข้อมลที่น่าเชื่อถือสำหรับการทำธุรกรรมแบบเพียร์ทูเพียร์ โดยลดตัวกลาง และเร่งกระบวนการดำเนินการ สามารถสร้างประโยชน์ต่อสังคมสูงสุดสำหรับการจัดส่งพลังงาน การจัดการธุรกรรม การจัดส่งพลังงาน และสนับสนุนการผลิตพลังงานทดแทน โดยมีการนำมาใช้ในการซื้อขายพลังงานในไมโครกริด และการบริหารจัดการพลังงานแบบแยกออกจากกัน การนำบล็อกเชนมาใช้ในภาคพลังงาน จำเป็นต้องคำนึงถึงเครื่องมือด้านพลังงานที่มีอยู่ และกรอบกฎหมายที่เกี่ยวข้องอย่างถึงพร้อม และต้องปรับปรุงให้เหมาะสมต่อการนำบล็อกเชนมาใช้ในภาคพลังงานได้อย่างกว้างขวาง [42]

อภิปรายและสรุปผล

ในบทความนี้ ได้ศึกษาแนวทางที่มีอยู่ในการจัดการกับความปลอดภัยจากการโจมตีทางไซเบอร์ในไมโครกริด ตามที่อธิบายไว้ข้างต้น ไมโครกริดโดยทั่วไปไม่มีแนวทางที่ยังไม่ชัดเจน ได้มีการใช้แบบจำลองไมโครกริด เพื่อการทดลองความปลอดภัยทางไซเบอร์ เนื่องจากมีบทบาทสำคัญในการนำไปสู่ไมโครกริดที่สมบูรณ์แบบ บริบทของไมโครกริดมักได้รับการพูดคุยกันในทางด้านวิชาการ อย่างไรก็ตามบทความนี้จะทำให้เราได้ศึกษาวิธีการ และวิธีแก้ปัญหาที่ออกแบบมาเป็นพิเศษซึ่งไม่จำเป็นต้องเหมาะกับทุกกรณี

มาตรการรักษาความปลอดภัยทางไซเบอร์สำหรับระบบพลังงานยังคงเป็นทางเลือก และไม่ใช่ข้อกำหนดที่บังคับให้ใช้ โดยเฉพาะอย่างยิ่งอุปกรณ์ที่เกี่ยวข้องกับระบบไฟฟ้าส่วนใหญ่ได้รับการพัฒนาอยู่ตลอดเวลา และมีการนำเครือข่ายอินเตอร์เน็ตมาประยุกต์ใช้ ทำให้กลไกการป้องกันทางไซเบอร์เป็นสิ่งจำเป็น และต้องพัฒนาไปควบคู่กับบริภัณฑ์ไฟฟ้าในระบบอย่างยิ่ง อย่างน้อยที่สุดการรักษาความปลอดภัยของไมโครกริดต้องใช้แนวทางแบบสหสาขาวิชาชีพ การพัฒนาทางเศรษฐกิจ และสังคมมักจะถูกละเลยในแง่มุมต่างๆ ในกระบวนการนี้ แม้แต่สิ่งประดิษฐ์ทางเทคโนโลยีที่โดดเด่นที่สุดก็ไม่มีประโยชน์หากไม่ได้รับการสนับสนุนจากผู้ที่มีส่วนรับผิดชอบ

กิตติกรรมประกาศ

งานวิจัยนี้ได้รับการสนับสนุนจากมหาวิทยาลัยพะเยา

เอกสารอ้างอิง

1. Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. Comput. Netw. 2013, 57, 1344–1371.
2. Rashid, M.H. Energy Systems in Electrical Engineering. In Smart Grids and Their Communication Systems; Kabalci, E., Kabalci, Y., Eds.; Springer: Singapore, 2019; pp. 1–644.
3. Leszczyna, R. Standards on cyber security assessment of smart grid. Int. J. Crit. Infrastruct. Prot. 2018, 22, 70–89.
4. Hossain, E. Communication Architectures and Models for Smart Grid. In Smart Grid Communications and Networking; Hossain, E., Han, Z., Poor, H.V., Eds.; Cambridge University Press: Cambridge, UK, 2012; pp. 1–103.
5. Prettico, M.; Flammini, G.; Andreadou, M.G.; Vitiello, N.; Fulli, S.; Masera, G. Distribution System Operators Observatory 2018: Overview of the Electricity Distribution System in Europe; Publications Office of the European Union: Ispra, Italy, 2019; pp. 1–77.
6. Prettico, G.; Gangale, F.; Mengolini, A.; Lucas, A.; Fulli, G. Distribution system operators from european electricity distribution systems to representative distribution networks. JRC Tech. Rep. Luxemb. 2018, 99, 273–280.
7. Yazdanian, M.; Mehrizi-Sani, A. Distributed control techniques in microgrids. IEEE Trans. Smart Grid 2014.
8. Sridhar, S.; Govindarasu, M. Model-based attack detection and mitigation for automatic generation control. IEEE Trans. Smart Grid 2014.
9. Chlela, M. Cyber Security Enhancement Against Cyber-Attacks on Microgrid Controllers; McGill University Montréal: Montréal, QC, Canada, 2017; pp. 1–177.
10. Knapp, E.D.; Samani, R. Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure, 1st ed.; Syngress: Rockland, MA, USA, 2013.
11. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State-of-the-art. Int. J. Electr. Power Energy Syst. 2017, 99, 45–56.
12. Lee, R.M.; Assante, M.J.; Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case.; E-ISAC: Washington, DC, USA, 2016; pp. 1–23.
13. Rekik,M.; Chtourou,Z.; Gransart,C.; Atieh,A.Acyber-physicalthreatanalysisformicrogrids. InProceedings of the 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD), Hammamet, Tunisia, 19–22 March 2018. Available online: https://ieeexplore.ieee.org/document/8570411 (accessed on 6 May 2020).
14. Liu, J.; Xiao, Y.; Gao, J. Achieving accountability in smart grid. IEEE Syst. J. 2014, 8, 493–508.
15. Srivastava, A.; Morris, T.; Ernster, T.; Vellaithurai, C.; Pan, S.; Adhikari, U. Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Trans. Smart Grid 2013, 4, 235–244.

16. Fooladivanda, D.; Hu, Q.; Chang, Y.H.; Sauer, P. Secure State Estimation and Control for Cyber Security of AC Microgrids. arXiv 2019, arXiv:1908.05843.
17. Esmalifalak, M.; Shi, G.; Han, Z.; Song, L. Bad data injection attack and defense in electricity market using game theory study. IEEE Trans. Smart Grid 2013, 4, 160–169.
18. Friedberg, I.; Laverty, D.; McLaughlin, F.; Smith, P. A Cyber-Physical Security Analysis of Synchronous-Islanded Microgrid Operation. In Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research 2015, Belfast, Swindon, UK, 17–18 September 2015.
19. Hayes, B.P. Distribution Generation Optimization and Energy Management. In Distributed Generation Systems; Gharehpetian, G.B., Agah, S.M.M., Eds.; Elsevier Inc.: Oxford, UK, 2017; pp. 415–451.
20. Lasseter, B. Microgrids distributed power generation. Power Eng. Soc. Winter Meet. 2001, 1, 146–149.
21. Lasseter, R. Microgrids. IEEE Power Eng. Soc. Winter Meet. 2002, 1, 305–308.
22. Katiraei, F.; Iravani, M.R. Power management strategies for a microgrid with multiple distributed generation units. IEEE Trans. Power Syst. 2006, 21, 1821–1831.
23. Olivares, D.E. Trends in microgrid control. IEEE Trans. Smart Grid 2014, 5, 1905–1919.
24. Buason, P.; Choi, H.; Valdes, A.; Liu, H.J. Cyber-physical systems of microgrids for electrical grid resiliency. ICPS 2019, 492–497.
25. Rana, M.M.; Li, L.; Su, S.W. Cyber attack protection and control of microgrids. IEEE/CAA J. Autom. Sin. 2018, 5, 602–609.
26. Peach, N.; Basseville, M.; Nikiforov, I.V. Detection of Abrupt Changes: Theory and Applications. J. R. Statal Soc. Ser. A (Stats in Soc.) 1993, 1, 185.
27. Jiao, Q.; Modares, H.; Lewis, F.L.; Xu, S.; Xie, L. Distributed L2-gain output-feedback control of homogeneous and heterogeneous systems. Automatica 2016, 71, 361–368.
28. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans. Control Netw. Syst. 2014, 1, 370–379.
29. Liu, S.; Wang, X.; Liu, P.X. Impact of communication delays on secondary frequency control in an islanded microgrid. IEEE Trans. Ind. Electron. 2015, 62, 2021–2031.
30. Hammad, E.; Farraj, A.; Kundur, D. Fundamental limits on communication latency for distributed control via electromechanical waves. IEEE Int. Conf. Commun. 2017.
31. Farraj, A.; Hammad, E.; Kundur, D. A systematic approach to delay: Adaptive control design for smart grids. IEEE Int. Conf. Smart Grid Commun. 2015, 768–773.
32. Guo, F. Comprehensive real-time simulation of the smart grid. IEEE Trans. Ind. Appl. 2013, 49, 899–908.
33. Cai, Y.; Li, Y.; Cao, Y.; Li, W.; Zeng, X. Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids. Int. J. Electr. Power Energy Syst. 2017, 89, 106–114.
34. Wang, Y.; Garnage, T.T.; Hauser, C.H. Security implications of transport layer protocols in power grid synchrophasor data communication. IEEE Trans. Smart Grid 2016, 7, 807–816.
35. Liu, S.; Liu, P.X.; Wang, X. Effects of cyber attacks on islanded microgrid frequency control. Proc. IEEE Int. Conf. Comput. Support. Coop. Work Des. 2016, 461–464.

36. Alhelou, H.; Golshan, M.E.; Hatziargyriou, N.D. Deterministic dynamic state estimation-based optimal lfc for interconnected power systems using unknown input observer. IEEE Trans. Smart Grid 2020, 11, 1582-1592.
37. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9-13 November 2009.
38. Dán, G.; Sandberg, H. Stealth attacks and protection schemes for state estimators in power systems. IEEE Int. Conf. Smart Grid Commun. 2010, 1-6.
39. Gallo, A.J.; Turan, M.S.; Nahata, P.; Boem, F.; Parisini, T.; Ferrari-Trecate, G. Distributed cyber-attack detection in the secondary control of dc microgrids. In Proceedings of the European Control Conference, Limassol, Cyprus, 12-15 June 2018. Available online: https://zenodo.org/record/2590092#.XzYHZzURXIU (accessed on 3 July 2020).
40. Hammad, E.; Ezeme, M.; Farraj, A. Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification. Int. J. Electr. Power Energy Syst. 2018, 104, 817-826.
41. Tellbach, D.; Li, Y.F. Cyber-attacks on smart meters in household nanogrid: Modeling, simulation and analysis. Energies 2018, 11, 316.
42. Hasse, F.; Von Perfall, A.; Hillebrand, T.; Smole, E.; Lay, M.; Charlet, L. Blockchain-an Opportunity for Energy Producers and Consumers Available online: https://asian-power.com/sites/default/files/asianpower/print/ AP_Novdec16_p44-45.pdf (accessed on 12 July 2020).

BIOGRAPHY

NAME	Satawat Muangchuen
DATE OF BIRTH	19 February 1991
PLACE OF BIRTH	Dok Kham Tai District, Phayao
INSTITUTIONS ATTENDED	2018 M.Eng. (Electrical Engineering), University of Phayao, Phayao 2010 B.Eng. (Electrical Engineering), University of Phayao, Phayao
HOME ADDRESS	266/7, Dok Kham Tai District, Phayao, 56120
PUBLICATION	1. S. Muangchuen, J. Pahasa, and I. Ngamroo. (2023). Improved Resilient Model Predictive Control for Enhanced Microgrid Virtual Inertia Emulation by Virtual Energy Storage System Under DoS Attacks. IEEE Access, 11, 96817 – 96830. doi: 10.1109/ACCESS.2023.3312608 2. S. Muangchuen, J. Pahasa, and C. Rakpenthai. (2024). Enhanced Resilient Model Predictive Control Electrolyzers for Frequency Regulations Under Severe Denial – of – Service Attacks. IEEE Access, 12, 65352 – 65361. doi: 10.1109/ACCESS.2024.3397874 3. ศตวรรษ เมืองชื่น, อิสระชัย งามหรู และ จงลักษณ์ พาหะซา. (2565). การควบคุมอินเวอร์เตอร์เครื่องปรับอากาศสำหรับเพิ่มแรงเฉื่อยเสมือนของไมโครกริด, การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 45, ภูสักธาร รีสอร์ท อำเภอเมือง จังหวัดนครนายก, 16 – 18 พฤศจิกายน พ.ศ. 2565.

4. ศตวรรษ เมืองชื่น, วิภารัตน์ ข่มอาวุธ, เชวศักดิ์ รักเป็นไทย และจงลักษณ์ พาหะซา. (2566). การควบคุมยานยนต์ไฟฟ้าเพื่อเพิ่มแรงเฉื่อยเสมือนของไมโครกริดที่มีแรงเฉื่อยเสมือนต่ำภายใต้การโจมตีแบบปฏิเสธการให้บริการ ด้วยตัวควบคุมพีไอดีแบบยืดหยุ่น. การประชุมวิชาการทางวิศวกรรมไฟฟ้าครั้งที่ 46, 15 – 17 พฤศจิกายน 2566

5. ศตวรรษ เมืองชื่น และจงลักษณ์ พาหะซา. (2566). ความปลอดภัยทางไซเบอร์ของไมโครกริด. การประชุมวิชาการพะเยาวิจัยครั้งที่ 13, 24 – 26 มกราคม 2567

AWARD RECEIVED –