Secure Sampled-data Observer-based Control for Wind Turbine Oscillation Under Cyber Attacks

Amir Amini, *Member, IEEE*, Mohsen Ghafouri, *Member, IEEE*, Arash Mohammadi, *Senior Member, IEEE*, Ming Hou, *Senior Member, IEEE*, Amir Asif, *Senior Member, IEEE*, and Konstantinos Plataniotis, *Fellow, IEEE*

***Abstract*—Inspired by the recent surge of interest in security analysis of renewable energies, this article proposes a cyber resilient control framework for large-scale wind parks (WPs) against denial of service (DoS) and deception attacks. A detailed cyber-physical model for a doubly-fed induction generator (DFIG)-based WP is first developed. It is shown that the WP is subject to a stability issue known as the sub-synchronous interaction (SSI). Additionally, two cyber threats in the forms of DoS and deception attack attempt to destabilize the WP from the subsynchronous perspective. To stabilize the WP under the SSI phenomenon and these cyber attacks, an observer-based fuzzy control scheme is proposed which requires only periodic samples of the output. Using a looped-Lyapunov functional (LLF) method for stability analysis, the control and observer gains are computed from the solution of some linear matrix inequality (LMI) conditions. The proposed design framework allows including the desired level of cyber resilience to DoS and deception attacks for computing proper control and observer gains. The effectiveness of the proposed controller against the considered threats is demonstrated via electromagnetic transient (EMT) simulations performed using the EMTP-RV software and a co-simulation platform.**

***Index Terms*–Large-scale wind park, cyber security, subsynchronous stability, denial of service attack, deception attack.**

I. Introduction

Recently, the deployment of wind-based energy generation units, particularly in the form of large-scale wind parks (WPs), has become a major paradigm in smart grids [1]. The use of these generation units is advantageous as they can harvest a huge amount of clean energy and replace the fossil fuel in future. Despite several technical difficulties, e.g., stability issues or intermittent nature, wind energy expansion almost doubled in 2020 compared to 2019 [2]. Among various wind turbine (WT) technologies, doubly-fed induction generators (DFIGs) are desirable in many applications due to the lower size of their converters and the ability to produce energy in a wide range of wind speeds. The ERCOT incident in 2009 and the Great Britain outage in 2019 [3] demonstrated that these energy units, if not controlled properly, are prone to stability issues. The cause of ERCOT incident received significant research as it introduced a new stability issue for WPs referred to as the sub-synchronous interaction (SSI). This phenomenon occurs when the DFIG-based WPs become radially connected to the commonly used series compensated transmission systems.

Following this incident, various mitigation techniques were proposed in the literature. Damping controllers received an overwhelming attention due to their simplicity and effectiveness [4]–[7]. The linear–quadratic regulator (LQR) technique is used in [4] to alleviate the unstable subsynchronous oscillations using an observer-based feedback controller. A two-degree-of-freedom control strategy with a damping control loop is proposed in [5] for mitigation of the SSI phenomenon which arises due to the induction generator effect. More recently, a variety of advanced control techniques are proposed in literature that investigate the SSI damping problem in different ways, e.g., data-driven adaptive method in [6], and μ-synthesis method in [7]. One common assumption in the above studies is the availability of infinite (continuous-time) measurement for control updates. In reality, however, digital measurement and control devices usually operate in a periodic manner and based on square clock signals. In control theory, sampled-data (periodic) techniques are usually employed which enable a digital implementation without approximation [8]–[11]. In [8], [9], the Lyapunov-Krasovskii functional (LKF) method is used to obtain stability conditions for the sampled-data systems. Since, large sampling intervals reduce the number of measurements, the upper bound of the sampling period is of great importance in sampled-data control design. In fact, a large allowable upper bound makes the implementation more efficient and reduces the conservatism of the design. Recently, the looped-Lyapunov functional (LLF) methods [10], [11] have received more attention due to their ability in reducing conservatism in the design of sampling period compared to the traditional LKF methods. To consider the impact of grid and WP uncertainties, robust control techniques are vastly used in literature [7]. The robust control method is most effective in small ranges

A. Amini is with the department of Electrical and Computer Engineering, Concordia University, Montreal, Canada.

M. Ghafouri, and A. Mohammadi are with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada.

M. Hou is with Toronto Research Centre, Defence Research and Development Canada, Toronto, Canada.

A. Asif is with the department of Electrical Engineering and Computer Science, York University, Toronto Canada.

K. Plataniotis is with the department of Electrical and Computer Engineering, University of Toronto, Toronto, Canada.

This Project was partially supported by the Department of National Defence's Innovation for Defence Excellence and Security (IDEaS) program, Canada.

of uncertainties. However, when a major change occurs in the grid or WP structure the uncertainties may exceed their expected bounds. Additionally, grid uncertainties often occur far away from the WP, and thus their impact is not easily observable by the WP operator. To tackle these issues, fuzzy controllers [12] that allow considering significant variation of grid parameters, outages of transmission lines, or grid maneuvers in the design stage are preferable. The use of sampled-data techniques (and in particular LLF), however, is not properly studied for WP and SSI stability analysis, especially in the presence of system uncertainties.

The mitigating controllers in a WP requires deployment of the information and communication technologies (ICTs). Similar to other smart grid domains, the use of these ICTs makes the WP vulnerable to cyber attacks due to the larger number of communication links [13]. The initial research in 2011 reported several vulnerabilities in the supervisory control and data acquisition (SCADA) systems of 2 megawatt WTs [14]. Despite these findings, for several years, wind-based energy units were assumed to be immune against cyber attacks. However, in March 2019 a WP in Salt Lake City, U.S., was the target of an attack which ceased the operator's control for around 500 megawatts of WTs [15]. The importance of the cyber security of wind energy units motivated the U.S. department of energy to focus on secure strategies to protect these units from cyber threats [15].

In general, denial of service (DoS) [16] and deception attacks (false data injection) [17] are two common types of adversarial actions on power and networked control systems. In DoS, the attacker attempts to delay, corrupt, or block certain communication channels in the power system. In a deception attack, the original signal is manipulated and injected in the system. As mentioned in [18], deception can occur in many forms such as additive attacks, min-max attacks, and scaling attacks on measurements and/or controller commands. An extensive amount of research has been conducted on detection of deception and DoS attacks [19], which is essential for ensuring secure operation and control of cyber physical systems (CPS). In addition to detection, mitigation-based strategies and resilient design are fundamental for system security. To mitigate the impact of deception attack on sensor and actuators in CPSs, an adaptive bound estimation mechanism is proposed in [20]. In [21], an additional observer is activated during the DoS attacks which estimates the controller values and helps in mitigating the overall effect of DoS. Focusing on deception attacks, a novel mitigation control scheme is proposed in [22], where a switching strategy prevents the attack signals injecting into the CPS and a state observer is designed to reconstruct the corrupted states. Resilient (secure) design often refers to the strategies that guarantee a certain level of tolerance to a particular type of attack by studying its impacts on the stability analysis and parameter design stage. In [23] and [24], secure strategies for the load frequency control in multi-area power systems are investigated under DoS and under deception attacks, respectively. A resilient PID controller is proposed in [25] where the data transmission from the controller to the actuator is susceptible to deception attacks. In [26], the reliability of a WP system is investigated against DoS attacks. However, the detection and mitigation of cyber threats against WPs mainly remained undiscussed in the literature. Despite the existing efforts, a resilient control framework that considers DoS or deception attacks in large-scale WP is yet to be investigated.

In summary, the following research gaps have been identified in the existing works related to the security of SSI damping controllers in WPs: (i) Existing SSI damping methods [4]–[7], [27] are based on continuous-time measurement and control update which is a restrictive assumption. (ii) With respect to the system security, the existing SSI damping schemes assume a healthy (attack-free) situation, which may not be operational in the presence of DoS and deception threats. (iii) The applicability of fuzzy controller for the SSI damping problem in DFIG-based WPs has not been fully studied. Motivated by the above discussions, this article proposes a resilient control scheme for large-scale WPs in the presence of DoS and deception attacks. The main contributions of the work are:

- Proposing a sampled-data control scheme based on the looped-Lyapunov functional technique which is suitable for digital implementation without approximation. This is in contrast to many existing SSI damping controller where the control scheme is based on the continuous-time measurement and control updates.
- Designing an SSI damping controller that guarantees a desired level of resilience to unknown DoS and/or deception attacks. In other words, our framework is able to include *a priori* level of resilience to DoS or deception attacks in the parameter design to proactively mitigate the impacts of potential adversaries in the form of DoS and/or deception.
- Developing a Takagi-Sugeno (T-S) fuzzy framework for the designed SSI damping controller to cope with the presence of uncertainty in the power grid.

Compared to our previous works [8], [13], this article fills a number of important research gaps. In [13], the possibility of internal scaling and external topology attacks are discussed and the ability of an observer-based detection scheme for attack identification is investigated. However, possible DoS attacks and design of resilient controller, and detailed stability analysis are missing in [13]. Moreover, the impact of substantial uncertainties on the performance of the attack mitigation scheme is neglected in [13]. This article aims to address these issues. Reference [8], which proposes a stabilization control scheme for linear systems under DoS, is based on three assumptions: (i) All system states are fully measurable, (ii) Uncertainty in model dynamics is negligible, and (iii) The adversary can only launch DoS attacks (not deception). All these strict assumptions are relaxed in this article. Additionally, the stability conditions in this article are obtained based on an

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3159582, IEEE Transactions on Smart Grid

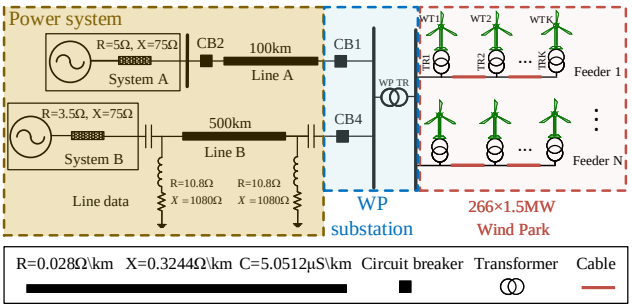

Fig. 1: Physical layer connection of a WP to a power system.

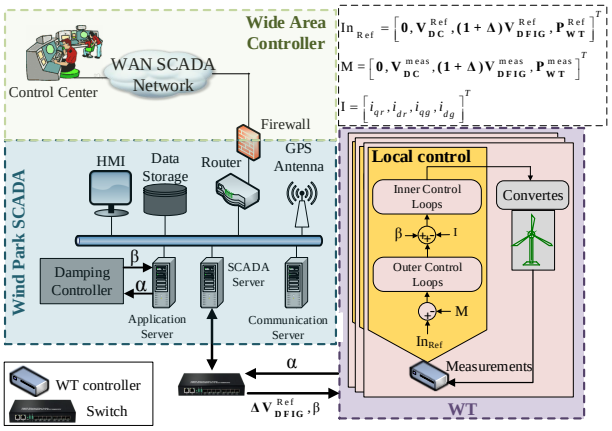

Fig. 2: Cyber layer connection of a WP to power system.

LLF criterion which is less conservative (in terms of larger allowable values for the sampling period and damping rate) than the LKF used in [8].

The article is organized as follows. Section II discusses the WP modeling and the problems to be studied. Section III formulates the problem. Section IV derives the main results to guarantee stability of the WP system under the given circumstances. Simulation studies are given in Section V. Lastly, Section VI concludes the article.

II. System Modeling and Problem Statement

The following notation is used in this article. $\|.\|$ stands for L_2 norm; $M>0$ indicates that matrix M is symmetric positive definite; I is the Identity matrix with proper order; 0 is the Zero matrix with proper order; $(.)^T$ is the transpose of the matrices or vectors; M^{-1} is the inverse of matrix M; $\text{sym}\{M\}=M+M^T$. The asterisk $*$ used in the block (j,i) of the symmetric matrices indicate the transpose of the (i,j) block.

Generic WPs are 'physically' connected to the electrical grid through a Point of Interconnection (PoI), which is basically a medium voltage (MV) to high voltage (HV) substation with transformers and controllers [4]. The WP often receives commands (e.g., the amount of required reactive power) from the grid operator. Additionally, the WP transmits measurements, such as the generated active power and voltage. These signals are communicated through the 'cyber layer' connections of the WP and gird. As such, the WPs have tangled cyber physical connection with the grid [13]. Thus, modeling of a grid-connected WP, particularly for cyber attack studies, requires detailed development of both layers at the same time.

A. Physical layer

The physical-layer connection of the considered WP to a power system is shown in Fig. 1. In this layer, the WP consists of 266 low-voltage WTs connected together through a medium-voltage collector grid. This collector grid transfers the power generation of WTs to the WP substation. The WP is connected to high-voltage grid at PoI. The power system consists of two transmission lines (Lines A and B), which connect the WP to other power grids (Systems A and B). Line A is a 100km short transmission line, whereas Line B is a 500km 50% compensated one [4], [28].

B. Cyber layer

The cyber-layer connection of the WP is shown in Fig. 2. The local control scheme of the WT uses the vector control techniques to regulate the DC link voltage, WT voltage, and power of turbine using its reference values, i.e., $(V_{\text{DC}}^{\text{Ref}})$, $((1+\Delta)V_{\text{DFIG}}^{\text{Ref}})$, and $(P_{\text{WT}}^{\text{Ref}})$, respectively. These parameters are gathered in vector In_{Ref} in Fig. 2. Since the reactive power of the grid side converter (GSC) is zero in practical applications, the corresponded value for this parameter is zero in In_{Ref}.

The control system of a DFIG has two decoupled control subsystems for the rotor side converter (RSC) and GSC as shown in Fig. 3. Using the vector control techniques, GSC and RSC are modeled in the dq-frame, where their corresponding signals are transferred to the stator voltage and flux reference frames, respectively. The q- and d-axis currents of the RSC (i_{qr} and i_{dr}) are utilized to, respectively, control the active power output and positive-sequence terminal voltage (P_{WT}^{ref} and V_{DFIG}^{ref}). The d-axis current of the GSC (i_{dg}) is used to regulate the DC bus voltage (V_{DC}) and the q-axis current of the GSC (i_{qg}) is used to support the grid with reactive power during faults. The value of the reference current for q-axis is zero in real applications [29], [30]. Both converters are controlled by a two-level controller. The slow outer control calculates the reference dq-frame currents and the fast inner control allows controlling the converter AC voltage reference. The reference for DFIG active power output (P_{WT}^{Ref}) is given by the maximum power point tracking (MPPT) algorithm. The reference for DFIG positive sequence voltage ($1+\Delta V_{DFIG}^{Ref}$) is calculated by the WP controller. During normal operation, GSC operates at unity power factor, i.e., $i_{qg}^{Ref}=0$, and the RSC controller prioritizes the active current. In the WT section, the control system receives a vector of set points In_{Ref} including (i) the reactive power component of the GSC, which is 0; (ii) the DC link voltage, which is regulated at V_{DC}^{Ref}; (iii) the voltage set point of each turbine, which is V_{DFIG}^{Ref} added by the amount ΔV_{DFIG}^{Ref} set by the central controller; and (iv) the active power generation of the WT P_{WT}^{Ref}, which is set by the MPPT of the WP controller. The difference between the measured parameters M and the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3159582, IEEE Transactions on Smart Grid

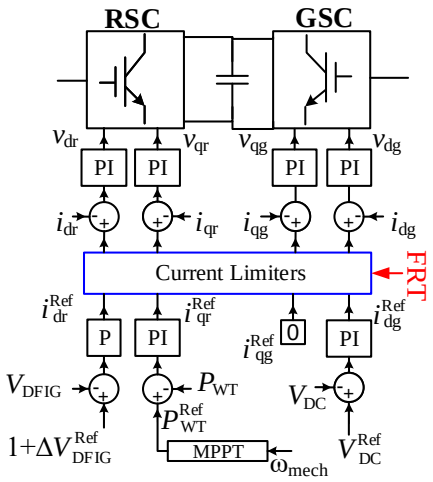

Fig. 3: The control system of a DFIG WT.

set point vector In_{Ref} is transmitted to the outer control loops to generate the reference points of the current $I^{Ref} = [i_{qr}^{Ref}, i_{dr}^{Ref}, i_{qg}^{Ref}, i_{dg}^{Ref}]^T$. The difference between these reference points and the measured converter currents $I = [i_{qr}, i_{dr}, i_{qg}, i_{dg}]^T$ are then transmitted to the fast inner loops of the WT. The WT controllers send α (which is the required signal for the SSI damping controller) to the damping controller through the communication switches and receive the control commands β from the controller. This β is added to the inner control loops of WT, which provides the most efficient controller performance. We note that the SSI phenomenon occurs when the WP is connected to a series compensated transmission system. This phenomenon is the result of a resonance between the controllers of the RSC and the grid at subsynchronous frequency range (i.e., < 60Hz) which is lower than the nominal grid frequency [4].

The attacks in this article include a set of situations in which the cyber system of the WP (Fig. 2) is compromised. The attacker intrudes into the WP SCADA system [31], [32] where the damping controller is located. The adversary aims to create a sustained or growing SSI oscillations leveraging the resonance between WP and its associated power system. The ways that an attacker can intrude into the system are categorized as: **(i)** The communication links between WTs and WP central controller that are used to transfer data related to the operation condition of the WTs, wind speed, mechanical torque, availability of the turbine, subsynchronous damping controller commands, etc. These communication links can be attacked by an adversary which has the capability to modify the IEC 104 data [13]. **(ii)** The WT and WP operations require a huge set of intelligent electronic devices (IEDs), e.g., controllers and relays. These IEDs can be attacked by malware or malicious software that aims to disrupt the operation of the WP. **(iii)** The cyber connection between the transmission grid operator and WP often increases the risk of cyber attacks. These connections that are mostly through the IEEE C37.188 protocols, lack the essential security requirements and can be leveraged by adversary to penetrate the WP cyber system.

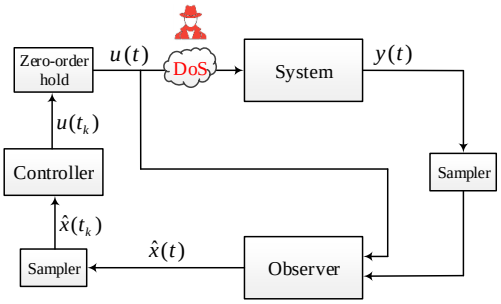

Fig. 4: The sampled-data observer-based scheme under DoS attack.

C. T-S fuzzy model for wind turbine system

The operating conditions for which a damping controller is designed may change due to uncertainty in power systems. Most of these uncertain conditions are within the WP (e.g., wind speed and generated reactive power). The impedance of the grid may also vary significantly and remain unnoticed by the WP operators. In such conditions and due to the wide range of uncertainty, the controller's performance degrades significantly. To tackle this issue, we deploy a T-S fuzzy technique based on the range of variations in the grid impedance. The described cyber-physical grid-connected WP is modeled with a T-S fuzzy state-space representation as:

Plant rule i: **IF** $\phi_i(t)$ is G_{i1}, ..., and $\phi_q(t)$ is G_{iq} **THEN**

$$\begin{aligned} \dot{\boldsymbol{x}}(t) &= A_i \boldsymbol{x}(t) + B_i \boldsymbol{u}(t), \\ \boldsymbol{y}(t) &= C_i \boldsymbol{x}(t), \end{aligned} \tag{1}$$

where $1 \le i \le r$ with i as the i-th fuzzy rule. Parameters $\phi_j(t)$ and G_{ij} for $1 \le i \le r$ and $1 \le j \le q$, respectively, denote the j-th premise variable and fuzzy set. Vector $\boldsymbol{x}(t) \in \mathbb{R}^n$ is the state variable. Matrices A_i, B_i, and C_i are constant and known, and represent the small signal behavior of the T-S fuzzy model. The details of these matrices can be found in [4]. Vector $\boldsymbol{u}(t) \in \mathbb{R}^m$ is the control scheme to be introduced shortly. It can be observed that A_i has a pair of unstable eigenvalues whose frequency is in the subsynchronous range. Let $\phi(t) = [\phi_1(t), \ldots, \phi_q(t)]$ and $g_i(\phi(t)) = \Pi_{j=1}^{q} G_{ij}(\phi_j(t))$. The membership function $\mu_i(\phi(t))$ is defined as:

$$\mu_i(\phi(t)) = \frac{g_i(\phi(t))}{\sum_{i=1}^{r} g_i(\phi(t))}. \tag{2}$$

Note that $0 \le \mu_i(\phi(t)) \le 1$ and $\sum_{i=1}^{r} \mu_i(\phi(t)) = 1$. The whole T-S fuzzy model can now be described as:

$$\begin{aligned} \dot{\boldsymbol{x}}(t) &= \sum_{i=1}^{r} \mu_i(\phi(t)) \Big\{ A_i \boldsymbol{x}(t) + B_i \boldsymbol{u}(t) \Big\}, \\ \boldsymbol{y}(t) &= \sum_{i=1}^{r} \mu_i(\phi(t)) C_i \boldsymbol{x}(t). \end{aligned} \tag{3}$$

As shown in Fig. 4, a sampler is employed to periodically measure the output of the system. We define the sampling instants as $\{t_k\}_{k \in \mathbb{N}_0}$. Following this notation, $\boldsymbol{x}(t_k)$ and $\boldsymbol{y}(t_k)$ are, respectively, the state and output values at time instant t_k. Let h denote the sampling period so that $t_{k+1} -$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3159582, IEEE Transactions on Smart Grid

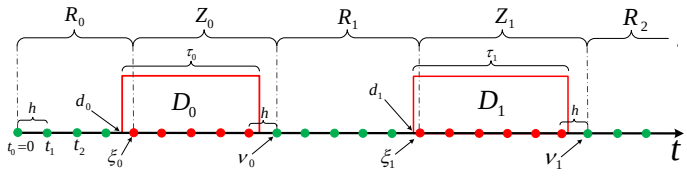

Fig. 5: An illustrative time diagram for two DoS intervals. Successful control updates are shown in green circles. Those update attempts that are denied due to DoS are in red.

$t_k = h$, $k \in \mathbb{N}_0$. To estimate the states of (3) based on $\boldsymbol{y}(t_k)$, the following T-S fuzzy observer is considered

$$\dot{\hat{\boldsymbol{x}}}(t) = \sum_{i=1}^{r} \mu_j(\phi(t)) \Big\{ A_i \hat{\boldsymbol{x}}(t) + B_i \boldsymbol{u}(t) + L_i(\boldsymbol{y}(t_k) - \hat{\boldsymbol{y}}(t_k)) \Big\},$$
$$\hat{\boldsymbol{y}}(t) = \sum_{i=1}^{r} \mu_i(\phi(t)) C_i \hat{\boldsymbol{x}}(t), \tag{4}$$

where $\hat{\boldsymbol{x}}(t) \in \mathbb{R}^n$ is the observer state vector and L_i, $1 \le i \le r$ are the observer gains which should be designed. The following T-S fuzzy observer-based feedback control scheme for the j-th rule is proposed to stabilize system (3)

Control Rule j: **IF** $\phi_1(t_k)$ is G_{i1}, ..., and $\phi_q(t_k)$ is G_{iq}, **THEN**

$$\boldsymbol{u}(t) = K_j \hat{\boldsymbol{x}}(t_k), \quad t \in [t_k, t_{k+1}), \tag{5}$$

where matrices $K_j \in \mathbb{R}^{m \times n}$, $(1 \le j \le r)$, are the control gains to be designed. Similar to (3), the overall fuzzy controller can be obtained

$$\boldsymbol{u}(t) = \sum\nolimits_{j=1}^{r} \mu_j(\phi(t)) K_j \hat{\boldsymbol{x}}(t_k), \quad t \in [t_k, t_{k+1}). \tag{6}$$

Remark 1. There are mainly three methods for digital control design [33]: **(i)** *Discretized synthesis*: where a discrete-time model is developed describing the system behavior at only sampling instants. Then, using the discrete-time control theory a digital controller is designed; **(ii)** *Continuous-based synthesis*: First, a continuous-time controller is designed for the system. The controller is then converted to a discrete model using some transformations; and **(iii)** *Sampled-data synthesis*: A digital controller is directly designed by considering the inter-sampling behavior. In the first method, the inter-sampling behavior is ignored in the synthesis. The second method depends on the accuracy of the transformation. The third method rules out any approximation and fully considers the inter-sampling behavior. Unlike [25] where a discretized synthesis is proposed, our design approach is based on the sampled-data synthesis with the above benefits.

D. Control Objectives

This article addresses the following questions: **Q1**. For given values of h (sampling period) and ζ (exponential rate of stabilization), how can we compute the required observer and SSI damping controller (5) so that the WP described in (3) is exponentially stable according to [34, Definition 2.1]? **Q2**. How to introduce a tuning parameter in the design stage so as to *proactively* control the resilience of the WP system to DoS attacks? **Q3**. How should the deception attacks be taken into account and develop a resilient framework to this type of adversary?

E. Denial of service attack

As mentioned previously, the DoS adversary blocks the control updates. The control scheme can be modeled as

$$\boldsymbol{u}(t) = \begin{cases} \sum_{j=1}^{r} \mu_j(\phi(t)) K_j \hat{\boldsymbol{x}}(t_k), & \text{DoS is inactive,} \\ 0, & \text{DoS is active.} \end{cases} \tag{7}$$

Similar to [35], the DoS is modeled in discrete intervals. This implies that the adversary has recurring *active* and *inactive* cycles. The c-th DoS attack interval is defined by

$$D_c = [d_c, d_c + \tau_c), \quad c \in \mathbb{N}_0. \tag{8}$$

Time instant d_c in (8) denotes the start of DoS interval D_c and τ_c is the duration of DoS in the c-th active interval. In Fig. 5, two schematic DoS intervals (D_0 and D_1) are shown. The union of DoS intervals in $[\,t_1, t_2\,)$ is given by

$$D(t_1, t_2) = \Big\{ \bigcup\nolimits_{c \in \mathbb{N}_0} D_c \Big\} \bigcap [\,t_1, t_2\,). \tag{9}$$

Those time intervals when DoS is inactive are called *healthy* intervals. The healthy intervals, which are the complement of the attack intervals, are given by

$$H(t_1, t_2) = [\,t_1, t_2\,) \setminus D(t_1, t_2). \tag{10}$$

Let $|D(t_1, t_2)|$ denote the accumulative length of DoS attacks between t_1 and t_2. With regards to the density of DoS, we denote $F(t_1, t_2)$ which returns the number of DoS off-to-on transitions in $[t_1, t_2)$. Conceptually speaking, $F(t_1, t_2)$ is a measure of how frequent the adversary launches DoS attacks.

Assumption 1. There exist positive constants α_0, α_1, β_0, and β_1 such that the following upper-bounds hold [35]

$$|\,D(t_1, t_2)\,| \le \alpha_0 + \frac{t_2 - t_1}{\alpha_1}, \quad \forall\, t_1, t_2 \in \mathbb{R}_{\ge 0},\ t_1 \le t_2, \tag{11}$$
$$\mathcal{F}(t_1, t_2) \le \beta_0 + \frac{t_2 - t_1}{\beta_1}, \quad \forall\, t_1, t_2 \in \mathbb{R}_{\ge 0},\ t_1 \le t_2. \tag{12}$$

Remark 2. Expressions (11) and (12) state that the strength of the DoS attacks, for any given t_1 and t_2, is proportional (with some coefficients) to the time difference. By the strength of attacks, we mean both the duration of DoS and its density. As indicated in [35], Assumption 1 reflects the energy-limited essence of the adversary. In fact, the adversary needs some inactive cycles to prolong its impact and last longer. On another note, expressions (11) and (12) in which no special pattern is considered for the attack duration and intensity, represent a more general case than the periodic one considered in [36].

F. Deception attack

In deception attack, the control signal $\boldsymbol{u}(t)$ is manipulated by both the additive and scaling factors [18]:

$$\boldsymbol{u}^{\mathcal{A}}(t) = (I + \Gamma(t))\boldsymbol{u}(t) + \boldsymbol{u}_s(t), \tag{13}$$

where $\Gamma(t) \in \mathbb{R}^{m\times m}$ is the time-varying scaling factor and $\boldsymbol{u}_s(t) \in \mathbb{R}^m$ is the additive deception signal. Excessive amounts of scaling attack can potentially lead to unstable behavior of the WP system (3). The attacker's objective in the additive deception is mainly to make the control system behave incorrectly. The attacker produces error in the control signal so that the system states deviate from their convergence equilibrium point. The following assumption is used for the severity of deception.

Assumption 2. *The following upper-bounds are considered for the deception attack parameters [25]*

$$0 \le \|\Gamma(t)\| \le \bar{\gamma}, \qquad \|\boldsymbol{u}_s(t)\| \le \bar{u}_s, \tag{14}$$

where $\bar{\gamma}$ and $\bar{u}_s$ are non-negative constants.

The boundedness of the attack signals [24], [25] represents the trade-off between the impact of attack and its stealthiness from the adversary viewpoint, i.e., although a large amplitude of deception may have more severe destructive impact on the system, but they could be easily detected by the security devices. If $\Gamma(t) = -I$ and $\boldsymbol{u}_s(t) = 0$, the deception attack alters to DoS. On another note, the WT controller converts the received measurement values to per unit. As such, the attack vector $\boldsymbol{u}_s(t)$ is also modeled in per unit, which implies that the entries in $\boldsymbol{u}_s(t)$ are normalized and comparable. The entries of vector $\boldsymbol{u}_s(t)$ are considered time-varying and can be independent of each other. This allows considering small or large values of additive attack for different components of the actual control signal $\boldsymbol{u}(t)$. The only condition on $\boldsymbol{u}_s(t)$ is its boundedness given in (14).

III. Problem Formulation

This section presents necessary notation to formulate the deception and DoS attacks. Moreover, the stability analysis of the closed-loop system under those attacks is pursued. Fig. 5 is given for visualization of different notation used to model DoS. In order to align the active and inactive DoS intervals with sampling instants t_k, we introduce a few variables as follows. Let $\xi_c = \min_{k\in\mathbb{N}_0}\{t_k \,|\, t_k > d_c\}$. Conceptually speaking, ξ_c is the next sample instant after d_c, which by definition is located inside D_c and thus the control update is denied. During D_c, the control scheme periodically attempts to update based on the earliest available measurement after DoS ends. Let $\nu_c = \min_{k\in\mathbb{N}_0}\{t_k \,|\, t_k > d_c + \tau_c\}$ specify the first successful control update after D_c. The c-th *effective* DoS interval is then defined by

$$Z_c = [\xi_c,\, \nu_c), \quad c \in \mathbb{N}_0.$$

In fact, there is practically no difference between Z_c and D_c in terms of the DoS impact on the system. Thus, for ease of analysis, we use the effective DoS interval Z_c. We define the union of effective DoS in interval $t \in [t_1, t_2]$ as

$$Z(t_1, t_2) = \bigcup\nolimits_{c\in\mathbb{N}_0} Z_c \cap [t_1, t_2]. \tag{15}$$

On the other hand, parameter

$$R(t_1, t_2) = \bigcup\nolimits_{c\in\mathbb{N}_0} R_c \cap [t_1, t_2], \tag{16}$$

is the union of healthy intervals. Parameters $|Z(t_1,t_2)|$ and $|R(t_1,t_2)|$, respectively, denote the total length of corresponding intervals for $t \in [t_1, t_2)$. We note that $R(t_1,t_2)$ and $Z(t_1,t_2)$ are complements of each other and the following expression holds true

$$|R(t_1,t_2)| = (t_2 - t_1) - |Z(t_1,t_2)|, \ \forall t_1, t_2 \ge 0,\ t_2 > t_1. \tag{17}$$

One can observe that $|Z_c| \le |D_c| + h$, $c \in \mathbb{N}_0$. This inequality can be observed in Fig. 5. Considering t_1 and t_2, the mentioned inequality leads to the following relation between $|Z(t_1,t_2)|$, $|D(t_1,t_2)|$, and $\mathcal{F}(t_1,t_2)$

$$|Z(t_1,t_2)| \le |D(t_1,t_2)| + h\mathcal{F}(t_1,t_2). \tag{18}$$

A. Closed-loop system

In this subsection, we obtain the closed-loop systems for the WP under 3 situations: (i) Attack free, (ii) Under DoS attacks, and (iii) under deception attacks. Let $\boldsymbol{e}(t) = \boldsymbol{x}(t) - \hat{\boldsymbol{x}}(t)$ denote the observer error at instant t. For notation brevity, we consider $\mu_i \triangleq \mu_i(\phi(t))$ and $\mu_j \triangleq \mu_j(\phi(t))$ for the remaining manuscript.

I. Attack free situation: Under the attack-free situation, the following closed-loop system for time interval $t \in [t_k, t_{k+1})$ is obtained from (3), (4), and (6)

$$\dot{\boldsymbol{x}}(t) = \sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i\mu_j\Big\{A_i\boldsymbol{x}(t) + B_iK_j(\boldsymbol{x}(t_k) + \boldsymbol{e}(t_k))\Big\}. \tag{19}$$

II. Under DoS attack: Considering (3), (4), and (7) the closed-loop system is given below

$$\dot{\boldsymbol{x}}(t) = \begin{cases} \sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i\mu_j\Big\{A_i\boldsymbol{x}(t) + B_iK_j(\boldsymbol{x}(t_k) + \boldsymbol{e}(t_k))\Big\}, & t \in R_m, \\ \sum_{i=1}^{r}\mu_iA_i\boldsymbol{x}(t), & t \in Z_m. \end{cases} \tag{20}$$

III. Under deception attack: The closed-loop system under this attack is obtained from (3), (4), (6), and (13)

$$\begin{aligned}\dot{\boldsymbol{x}}(t) = \sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i\mu_j\Big\{&A_i\boldsymbol{x}(t) + B_iK_j(\boldsymbol{x}(t_k) + \boldsymbol{e}(t_k)) \\ &+ \Gamma(t)B_iK_j\left(\boldsymbol{x}(t_k) + \boldsymbol{e}(t_k)\right) + B_i\boldsymbol{u}_s(t_k)\Big\}.\end{aligned} \tag{21}$$

IV. Under both DoS and deception attacks: The closed-loop system in this scenario is

$$\dot{\boldsymbol{x}}(t) = \begin{cases} \sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i\mu_j\Big\{A_i\boldsymbol{x}(t) + B_iK_j(\boldsymbol{x}(t_k) + \boldsymbol{e}(t_k)) \\ +\Gamma(t)B_iK_j\left(\boldsymbol{x}(t_k) + \boldsymbol{e}(t_k)\right) + B_i\boldsymbol{u}_s(t_k)\Big\}, & t \in R_m, \\ \sum_{i=1}^{r}\mu_iA_i\boldsymbol{x}(t), & t \in Z_m. \end{cases} \tag{22}$$

In all the above cases, it holds that

$$\dot{\boldsymbol{e}}(t)=\sum_{i=1}^{r}\mu_i\Big\{A_i-L_iC_i\Big\}\boldsymbol{e}(t). \tag{23}$$

IV. Main results

This section studies stability conditions for the WP under different scenarios discussed in Section III-A.

A. Parameter synthesis: the attack free situation

We first consider an attack-free situation, i.e., no DoS and no deception attacks occur during the operation.

Theorem 1. Design observer gains L_i such that $A_{L_i}=A_i-L_iC_i$ is Hurwitz stable for $(1\le i\le r)$. Tune the desired damping rate ζ_1 and sampling period h as initial parameters. Let $\alpha=e^{-2\zeta_1 h}$. If there exist the following decision variables

- $n\times n$ dimensional positive definite matrices P_1, P_3, W and $2n\times 2n$ dimensional symmetric matrix P_2,
- any real-valued matrices $M_{n\times 5n}$, $N_{n\times 5n}$, $G_{n\times n}$, and $X_{i_{m\times n}}$, $(1\le i\le r)$;

such that the following LMIs are satisfied

$$S_{ii}<0,\quad i=1,\dots,r \tag{24}$$

$$\frac{2}{r-1}S_{ii}+S_{ij}+S_{ji}<0,\quad 1\le i\ne j\le r \tag{25}$$

$$U_{ii}<0,\quad i=1,\dots,r \tag{26}$$

$$\frac{2}{r-1}U_{ii}+U_{ij}+U_{ji}<0,\quad 1\le i\ne j\le r \tag{27}$$

then, the following gains K_i stabilize system (19)

$$K_i=X_i(G^{-1})^T,\quad (1\le i\le r). \tag{28}$$

Undefined parameters in (24)-(27) are given below

$$\begin{aligned}
S_{ij}&=\Theta_{ij,1}+\Theta_2+h\Theta_3,\\
U_{ij}&=\begin{bmatrix}\Theta_{ij,1}+\Theta_2 & \sqrt{\alpha h}M^T & h\sqrt{\alpha h}N^T\\ * & -P_3 & 0\\ * & * & -3P_3\end{bmatrix},\\
\Theta_{ij,1}&=\mathrm{sym}\{E_5^TQ_{ij}\},\\
\Theta_2&=\mathrm{sym}\{J_1^TP_1J_4+\alpha M^TE_3-2\alpha N^TJ_3+\alpha hN^TE_4\}\\
&\quad-E_1^TP_2E_1-J_5^TWJ_5+2\zeta_1J_1^TP_1J_1,\\
\Theta_3&=\mathrm{sym}\{E_2^TP_2E_1\}+J_4^TP_3J_4+2\zeta_1E_1^TP_2E_1,\\
J_k&=\begin{bmatrix}0_{n\times(k-1)n} & I_n & 0_{n\times(5-k)n}\end{bmatrix},\ k=1,2,...,5,\\
Q_{ij}&=-G^TJ_4+A_iG^TJ_1+B_iX_jE_6,\\
E_1&=\begin{bmatrix}J_1-J_2\\ J_3\end{bmatrix},\ E_2=\begin{bmatrix}J_4\\ J_1\end{bmatrix},\ E_3=J_1-J_2,\\
E_4&=J_1+J_2,\quad E_5=J_1+J_2+J_4,\quad E_6=J_2+J_5.
\end{aligned}$$

Proof. With matrices $\tilde{P}_1>0,\tilde{P}_3>0$, and symmetric $\tilde{P}_2$, we choose the LLF $V=V_1+V_2+V_3$ for $t\in[t_k,t_{k+1}]$ where

$$V_1=\boldsymbol{x}^T(t)\tilde{P}_1\boldsymbol{x}(t), \tag{29a}$$

$$V_2=(t_{k+1}-t)\boldsymbol{\phi}_1^T\tilde{P}_2\boldsymbol{\phi}_1, \tag{29b}$$

$$V_3=(t_{k+1}-t)\int_{t_k}^{t}e^{2\zeta_1(\lambda-t)}\dot{\boldsymbol{x}}^T(\lambda)\tilde{P}_3\dot{\boldsymbol{x}}(\lambda)d\lambda, \tag{29c}$$

where $\boldsymbol{\phi}_1=[\boldsymbol{x}^T(t)-\boldsymbol{x}^T(t_k),\ \int_{t_k}^{t}\boldsymbol{x}^T(\lambda)d\lambda]^T$. Let $\boldsymbol{\phi}_2=[\boldsymbol{x}^T(t),\ \boldsymbol{x}^T(t_k),\ \int_{t_k}^{t}\boldsymbol{x}^T(\lambda)d\lambda,\ \dot{\boldsymbol{x}}^T(t),\ \boldsymbol{e}^T(t_k)]^T$. We obtain the time derivative of (29) as follows

$$\begin{aligned}
\dot{V}\le\boldsymbol{\phi}_2^T\Big(&\mathrm{sym}\{J_1^T\tilde{P}_1J_4\}-E_1^T\tilde{P}_2E_1\\
&+(t_{k+1}-t)\left(\mathrm{sym}\{E_2^T\tilde{P}_2E_1\}+J_4^T\tilde{P}_3J_4\right)\Big)\boldsymbol{\phi}_2\\
&-\textstyle\int_{t_k}^{t}e^{2\zeta_1(\lambda-t)}\dot{\boldsymbol{x}}^T(\lambda)\tilde{P}_3\dot{\boldsymbol{x}}(\lambda)d\lambda-2\zeta_1(t_{k+1}-t)V_3.
\end{aligned} \tag{30}$$

Let $\alpha=e^{-2\zeta_1 h}$. From [37, Lemma 1], we have the following inequality for free matrices $\bar{M}_{n\times 6n}$ and $\bar{N}_{n\times 6n}$

$$\begin{aligned}
&-\textstyle\int_{t_k}^{t}e^{2\zeta_1(\lambda-t)}\dot{\boldsymbol{x}}^T(\lambda)\tilde{P}_3\dot{\boldsymbol{x}}(\lambda)d\lambda\le-\alpha\int_{t_k}^{t}\dot{\boldsymbol{x}}^T(\lambda)\tilde{P}_3\dot{\boldsymbol{x}}(\lambda)d\lambda\\
&\le\boldsymbol{\phi}_2^T\Big((t-t_k)\alpha\Big(\tilde{M}^T\tilde{P}_3^{-1}\tilde{M}+\frac{h^2}{3}\tilde{N}^T\tilde{P}_3^{-1}\tilde{N}\Big)\\
&+\mathrm{sym}\Big\{\alpha\tilde{M}^TE_3-2\alpha\tilde{N}^TJ_3+(t-t_k)\alpha\tilde{N}^TE_4\Big\}\Big)\boldsymbol{\phi}_2.
\end{aligned} \tag{31}$$

From (23), the following expression holds for $\bar{W}>0$

$$-\boldsymbol{e}^T(t_k)\bar{W}\boldsymbol{e}(t_k)+\boldsymbol{b}^T(t_k)\bar{W}\boldsymbol{b}(t_k)=0, \tag{32}$$

where $\boldsymbol{b}(t)=\exp(\int_0^t\sum_{i=1}^{r}\mu_i\{A_i-L_iC\}dt)\boldsymbol{e}(0)$. The following null equation holds true from (19)

$$\begin{aligned}
&2\Big(\boldsymbol{x}^T(t)+\dot{\boldsymbol{x}}^T(t)+\boldsymbol{x}^T(t_k)\Big)G^{-1}\Big(-\dot{\boldsymbol{x}}(t)\\
&+\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i\mu_j\Big\{A_i\boldsymbol{x}(t)+B_iK_j(\boldsymbol{x}(t_k)+\boldsymbol{e}(t_k))\Big\}\Big)=0.
\end{aligned} \tag{33}$$

Next, we obtain sufficient conditions for stability of (19). Under condition $t_{k+1}-t\le 1$, the following inequality holds

$$\dot{V}+2\zeta_1(V_1+V_2)+2\zeta_1(t_{k+1}-t)V_3\le\dot{V}+2\zeta_1V. \tag{34}$$

Thus, if the right hand side of (34) is negative definite, the left hand side is also negative definite. Combining the expressions from (30) to (32), the following is obtained

$$\dot{V}+2\zeta_1V\le\boldsymbol{\phi}_2^T\tilde{\Theta}\boldsymbol{\phi}_2+\boldsymbol{b}^T(t_k)\bar{W}\boldsymbol{b}(t_k), \tag{35}$$

where

$$\begin{aligned}
\tilde{\Theta}&=\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i\mu_j\tilde{\Theta}_{ij,1}+\tilde{\Theta}_2+(t_{k+1}-t)\tilde{\Theta}_3+(t-t_k)\tilde{\Theta}_4,\\
\tilde{\Theta}_{ij,1}&=\mathrm{sym}\{E_5^TG^{-1}\tilde{Q}_{ij}\},\\
\tilde{\Theta}_2&=\mathrm{sym}\{J_1^T\tilde{P}_1J_4+\alpha\tilde{M}^TE_3-2\alpha\tilde{N}^TJ_3\}-E_1^T\tilde{P}_2E_1\\
&\quad-J_5^T\tilde{W}J_5+2\zeta_1J_1^T\tilde{P}_1J_1,\\
\tilde{\Theta}_3&=\mathrm{sym}\{E_2^T\tilde{P}_2E_1\}+J_4^T\tilde{P}_3J_4+2\zeta_1E_1^T\tilde{P}_2E_1,\\
\tilde{\Theta}_4&=\alpha\left(\mathrm{sym}\{\tilde{N}^TE_4\}+\tilde{M}^T\tilde{P}_3^{-1}\tilde{M}+\frac{h^2}{3}\tilde{N}^T\tilde{P}_3^{-1}\tilde{N}\right),\\
\tilde{Q}_{ij}&=A_iJ_1+B_iK_jE_6-J_4.
\end{aligned}$$

If $\tilde{\Theta}<0$, then the following can be obtained from (35)

$$V(t)\le e^{-2\zeta_1 t}V(0)+c(t_k), \tag{36}$$

where $c(t_k)=\frac{1}{2\zeta_1}\boldsymbol{b}^T(t_k)\bar{W}\boldsymbol{b}(t_k)$. Note that A_i-L_iC is Hurwitz stable and thus $c(t_k)$ in (36) asymptotically approaches zero. Recall that expression (36) is derived under

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3159582, IEEE Transactions on Smart Grid

condition $\tilde{\Theta} < 0$. By the convex combination method [38], inequality $\tilde{\Theta} < 0$ holds for any $t \in [t_k, t_{k+1})$, if and only if

$$\tilde{S} \triangleq \sum_{i=1}^{r}\sum_{j=1}^{r} \mu_i\mu_j \tilde{\Theta}_{ij,1} + \tilde{\Theta}_2 + h\tilde{\Theta}_3 < 0, \tag{37}$$

$$\tilde{U} \triangleq \sum_{i=1}^{r}\sum_{j=1}^{r} \mu_i\mu_j \tilde{\Theta}_{ij,1} + \tilde{\Theta}_2 + h\tilde{\Theta}_4 < 0. \tag{38}$$

Applying the Schur complement lemma, it is easy to see that (38) is equivalent to the following condition

$$\hat{U} \triangleq \sum_{i=1}^{r}\sum_{j=1}^{r} \mu_i\mu_j \begin{bmatrix} \hat{U}_{ij,1} & \sqrt{\alpha h}\tilde{M}^T & \sqrt{\alpha h}h\tilde{N}^T \\ * & -\tilde{P}_3 & 0 \\ * & * & -3\tilde{P}_3 \end{bmatrix} < 0,$$

where $\hat{U}_{ij,1} = \tilde{\Theta}_{ij,1} + \tilde{\Theta}_2 + \alpha \times \mathrm{sym}\{\tilde{N}^T E_4\}$. Let $\Lambda_1 = I_5 \otimes G$ and $\Lambda_2 = I_7 \otimes G$. We pre- and post-multiply $\tilde{S}$ in (37) by Λ_1 and Λ_1^T to obtain $\bar{S} \triangleq \Lambda_1 \tilde{S} \Lambda_1^T$. In a similar fashion, we define $\bar{U} \triangleq \Lambda_2 \hat{U} \Lambda_2^T$. Now, define the following alternative variables $X_i = K_i G^T$, $i = 1, \ldots, r$, $P_1 = G\tilde{P}_1 G^T$, $P_3 = G\tilde{P}_3 G^T$, $W = G\tilde{W} G^T$, $P_2 = (I_2 \otimes G)\tilde{P}_2 (I_2 \otimes G^T)$, $M = G\tilde{M}\Lambda_1^T$, $N = G\tilde{N}\Lambda_1^T$. We replace these alternative variables in $\bar{S}$ and $\bar{U}$ and label the resulting matrices as S and U, respectively. According to [39, Theorem 2.2], condition $S < 0$ is fulfilled if $S_{ii} < 0$ and $\frac{2}{r-1}S_{ii} + S_{ij} + S_{ji} < 0$. These conditions are given in (24) and (25). The same statement is true for U, which gives way to the LMIs given in (26) and (27). Control gains K_i, $i = 1, \ldots, r$, are computed from (28). This completes the proof. □

Remark 3. As mentioned in [10], [11], the LLF-based stability methods ensure a less conservative solution (in terms of larger allowable values for the sampling period and damping rate) than traditional Lyapunov functionals [8], [9]. The main reason is that the LLF methods relax some of the constraints on the positive definiteness of the functionals. For example, the LKF in [8], [9] has the form of $V = \boldsymbol{x}^T(t)\tilde{P}_1\boldsymbol{x}(t) + \int_{t-h}^{t} e^{\zeta_1(s-t)}\boldsymbol{x}^T(s)\tilde{P}_2\boldsymbol{x}(s)ds + h\int_{-h}^{0}\int_{t+s}^{t} e^{\zeta_1(v-t)}\dot{\boldsymbol{x}}^T(v)\tilde{P}_3\dot{\boldsymbol{x}}(v)dvds$, which is constrained on $\tilde{P}_i > 0$ for all $i = 1, 2, 3$. In contrast, the LLF in (29) does not require $\tilde{P}_2$ to be positive definite. As compared in [10, Table I], this reduces the conservatism of the solution without compromising the computational complexity.

B. Parameter synthesis: in the presence of DoS attack

On the basis of Theorem 1, we develop the following theorem which computes proper control gains and specifies the level of resilience to DoS attacks.

Theorem 2. Design observer gains L_i so that $A_{L_i} = A_i - L_i C_i$ is Hurwitz stable for $(1 \le i \le r)$. Tune the desired damping rate ζ_1, sampling period h, and DoS resilience level $\Omega < 1$ as initial parameters. If there exist the set of decision variables given in Theorem 1 (i.e., P_1, P_2, P_3, W, M, N, G, X_i) such that the following LMIs are satisfied

$$S_{ii} < 0, \quad i = 1, \ldots, r \tag{39}$$

$$\frac{2}{r-1}S_{ii} + S_{ij} + S_{ji} < 0, \quad 1 \le i \ne j \le r \tag{40}$$

$$U_{ii} < 0, \quad i = 1, \ldots, r \tag{41}$$

$$\frac{2}{r-1}U_{ii} + U_{ij} + U_{ji} < 0, \quad 1 \le i \ne j \le r \tag{42}$$

$$\Psi_{i,1} + \Psi_2 + h\Psi_3 < 0, \quad i = 1, \ldots, r \tag{43}$$

then, the control gains are computed from

$$K_i = X_i (G^{-1})^T, \quad (1 \le i \le r). \tag{44}$$

Using the above control gains guarantees stability of system (20) under DoS attacks with the following strength

$$\frac{1}{\alpha_1} + \frac{h}{\beta_1} < \Omega. \tag{45}$$

Unknown parameters in (39), (40), (41), and (42) are previously given in Theorem 1. Unknown parameters in (43) are defined below

$$\begin{aligned}
&\Psi_{i,1} = \mathrm{sym}\{\mathcal{E}_3^T \mathcal{Q}_i\},\\
&\Psi_2 = \mathrm{sym}\{\mathcal{J}_1^T P_1 \mathcal{J}_4\} - \mathcal{E}_1^T P_2 \mathcal{E}_1 - 2\zeta_2 \mathcal{J}_1^T P_1 \mathcal{J}_1,\\
&\Psi_3 = \mathrm{sym}\{\mathcal{E}_2^T P_2 \mathcal{E}_1\} + \mathcal{J}_4^T P_3 \mathcal{J}_4 - 2\zeta_2 \mathcal{J}_1^T P_2 \mathcal{J}_1,\\
&\mathcal{Q}_i = -G^T \mathcal{J}_4 + A_i G^T \mathcal{J}_1,\\
&\mathcal{J}_k = \begin{bmatrix} 0_{n\times(k-1)n} & I_n & 0_{n\times(4-k)n} \end{bmatrix}, \ k = 1, 2, ..., 4,\\
&\mathcal{E}_1 = \begin{bmatrix} \mathcal{J}_1 - \mathcal{J}_2 \\ \mathcal{J}_3 \end{bmatrix}, \ \mathcal{E}_2 = \begin{bmatrix} \mathcal{J}_4 \\ \mathcal{J}_1 \end{bmatrix}, \quad \mathcal{E}_3 = \mathcal{J}_1 + \mathcal{J}_2 + \mathcal{J}_4,\\
&\zeta_2 = \frac{\zeta_1(1-\Omega)}{\Omega}.
\end{aligned}$$

Proof. In the presence of DoS, the system is either in Healthy intervals ($t \in R_m$) or in Attack intervals ($t \in Z_m$). The proof follows in 3 steps.

Step I. Healthy intervals ($t \in R_m$): From Theorem 1 we previously showed that if LMIs (24) to (27) are guaranteed then trajectories of the system follows (35) which is reproduced below for ease of reference

$$\dot{V}(t) < -2\zeta_1 V(t) + \boldsymbol{b}^T(t_k)\bar{W}\boldsymbol{b}(t_k), \quad t \in R_m. \tag{46}$$

Step II. DoS intervals ($t \in Z_m$): If $t \in Z_m$, the states of (20) may diverge. There exists a divergence rate $\zeta_2 > 0$ such that

$$\dot{V}(t) < 2\zeta_2 V(t), \quad t \in Z_m. \tag{47}$$

where $V = V_1 + V_2 + V_3$ is given in (29). We expand (47) as

$$\dot{V} - 2\zeta_2 V \le \dot{V} - 2\zeta_2(V_1 + V_2) < 0. \tag{48}$$

Let $\boldsymbol{\phi}_3 = [\boldsymbol{x}^T(t), \boldsymbol{x}^T(t_k), \int_{t_k}^{t}\boldsymbol{x}^T(\lambda)d\lambda, \dot{\boldsymbol{x}}^T(t)]^T$. The following holds for the derivatives of $V(t)$ in $t \in Z_m$

$$\begin{aligned}
\dot{V} \le \boldsymbol{\phi}_3^T \Big(&\mathrm{sym}\{\mathcal{J}_1^T \tilde{P}_1 \mathcal{J}_4\} - \mathcal{E}_1^T \tilde{P}_2 \mathcal{E}_1 \\
&+ (t_{k+1} - t)\left(\mathrm{sym}\{\mathcal{E}_2^T \tilde{P}_2 \mathcal{E}_1\} + \mathcal{J}_4^T \tilde{P}_3 \mathcal{J}_4\right)\Big)\boldsymbol{\phi}_3.
\end{aligned} \tag{49}$$

The following null equality holds based on (20) for $t \in Z_m$

$$2\Big(\boldsymbol{x}^T(t) + \dot{\boldsymbol{x}}^T(t) + \boldsymbol{x}^T(t_k)\Big)G^{-1}\Big(\sum_{i=1}^{r}\mu_i A_i \boldsymbol{x}(t) - \dot{\boldsymbol{x}}(t)\Big) = 0. \tag{50}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3159582, IEEE Transactions on Smart Grid

Considering (49) and (50), we revise (48) as follows

$$\dot{V} - 2\zeta_2(V_1 + V_2) = \boldsymbol{\phi}_3^T \tilde{\Psi} \boldsymbol{\phi}_3 < 0, \tag{51}$$

where

$$\tilde{\Psi} = \sum_{i=1}^{r} \mu_i \tilde{\Psi}_{i,1} + \tilde{\Psi}_2 + (t_{k+1} - t)\tilde{\Psi}_3, \tag{52}$$

with $\tilde{\Psi}_{i,1} = \text{sym}\{\mathcal{E}_3^T G^{-1} \tilde{\mathcal{Q}}_i\}$, $\tilde{\Psi}_2 = \text{sym}\{\mathcal{J}_1^T \tilde{P}_1 \mathcal{J}_4\} - \mathcal{E}_1^T \tilde{P}_2 \mathcal{E}_1 - 2\zeta_2 \mathcal{J}_1^T \tilde{P}_1 \mathcal{J}_1$ $\tilde{\Psi}_3 = \text{sym}\{\mathcal{E}_2^T \tilde{P}_2 \mathcal{E}_1\} + \mathcal{J}_4^T \tilde{P}_3 \mathcal{J}_4 - 2\zeta_2 \mathcal{J}_1^T \tilde{P}_2 \mathcal{J}_1$, and $\tilde{\mathcal{Q}}_i = A_i \mathcal{J}_1 - \mathcal{J}_4$. Considering (48) and (51), if $\tilde{\Psi} < 0$ then $\dot{V}(t) - 2\zeta_2 V(t) < 0$ is guaranteed for $t \in Z_m$. We pre- and post multiply $\tilde{\Psi}$ by Λ_3 and Λ_3^T, where $\Lambda_3 = I_4 \otimes G$. Employing the same alternative variables used at the end of proof of Theorem 1 leads to the LMI given in (43).

Step III. Merging healthy and DoS intervals: Now, we merge (46) and (47) to obtain the *overall* stability condition and the maximum tolerable amount of DoS. Expressions (46) and (47) are expanded as follows

$$V(t) \le e^{-2\zeta_1(t-\nu_{m-1})} V(\nu_{m-1}) + c(t_k), \quad t \in R_m, \tag{53}$$

$$V(t) \le e^{2\zeta_2(t-\xi_m)} V(\xi_m), \quad t \in Z_m. \tag{54}$$

where $c(t_k) = \frac{\boldsymbol{b}^T(t_k) \bar{Q} \boldsymbol{b}(t_k)}{2\zeta_1}$. Assume that $t \in Z_m$. From (53) and (54) we obtain that [1]

$$\begin{aligned} V(t) &\le e^{2\zeta_2(t-\xi_m)} V(\xi_m) \\ &\le e^{2\zeta_2(t-\xi_m)} \left(e^{-2\zeta_1(\xi_m - \nu_{m-1})} V(\nu_{m-1}) + c(t_k) \right) \\ &\le e^{2\zeta_2(t-\xi_m)} e^{-2\zeta_1(\xi_m - \nu_{m-1})} e^{2\zeta_2(\nu_{m-1} - \xi_{m-1})} V(\xi_{m-1}) \\ &\quad + c(t_k)\, e^{2\zeta_2(t-\xi_m)} \\ &\le \dots \\ &\le e^{-2\zeta_1 |R(0,t)|} e^{2\zeta_2 |Z(0,t)|} V(0) \\ &\quad + \bar{c} \sum_{\substack{m \in \mathbb{N}_0 \\ \xi_m \le t}} e^{-2\zeta_1 |R(\nu_{m-1},t)|} e^{2\zeta_2 |Z(\xi_m,t)|}, \end{aligned} \tag{55}$$

where $\bar{c} = \max_{k \in \mathbb{N}_0} \{c(t_k)\}$. It is straightforward to show that (55) also holds if we start with $t \in R_m$. From (11), (12), (17), and (18), we derive that

$$e^{-2\zeta_1 |R(0,t)|} e^{2\zeta_2 |Z(0,t)|} \le \rho^2\, e^{-2\zeta t}, \tag{56}$$

where

$$\rho = e^{(\zeta_1 + \zeta_2)(\alpha_0 + h\beta_0)}, \quad \zeta = \zeta_1 - (\zeta_1 + \zeta_2)\left(\frac{1}{\alpha_1} + \frac{h}{\beta_1} \right). \tag{57}$$

Condition (56) leads to

$$V(t) < \rho^2 e^{-2\zeta t} V(0) + \eta, \quad t \ge 0, \tag{58}$$

where $\eta = \bar{c} \sum_{\substack{m \in \mathbb{N}_0 \\ \xi_m \le t}} e^{-2\zeta_1 |R(\nu_{m-1},t)|} e^{2\zeta_2 |Z(\xi_m,t)|}$. Based on (58), if $\zeta > 0$ then the system remains stable under DoS attacks. This implies that the DoS attacks should satisfy $(\frac{1}{\alpha_1} + \frac{h}{\beta_1}) < \Omega$ with $\Omega = \zeta_1/(\zeta_1 + \zeta_2)$. Parameter Ω is referred to as the DoS resilience, since it represents the upper-bound for tolerable amount of DoS. Note that with $\zeta > 0$ and $A_{L_i} = A_i - L_i C$ being Hurwitz stable, parameter η approaches zero asymptotically. This completes the proof. □

[1] For visualization of inequalities in (55) refer to Fig. 5.

Remark 4. As mentioned in Theorem 2, parameter Ω is the desired resilience level to DoS that guarantees stable performance for system (19) under DoS satisfying $\frac{1}{\alpha_1} + \frac{h}{\beta_1} < \Omega$. Parameter $\frac{1}{\alpha_1} + \frac{h}{\beta_1}$ is a joint term that includes both the '*average time ratio of DoS*', (i.e., $\frac{1}{\alpha_1}$), and the '*average density of attacks*', (i.e., $\frac{1}{\beta_1}$). Since the density of DoS is scaled by h, the impact of $\frac{1}{\alpha_1}$ in $\frac{1}{\alpha_1} + \frac{h}{\beta_1}$ is more dominant than $\frac{h}{\beta_1}$, especially for small values of h. Therefore, the above condition can roughly be reduced to $\frac{1}{\alpha_1} < \Omega$. For example, choosing $\Omega = 0.1$ in Theorem 2 means that a $\frac{1}{\alpha_1} \approx 0.1$ fraction of DoS attacks to total time is tolerated. In other words, stability of the system is guaranteed if DoS intervals do not occupy around more that 10% of the total operating time. It is clear that higher values for Ω, by definition, guarantees resilience to a more intense DoS. However, with higher values for Ω, parameter $\zeta_2 = \frac{\zeta_1(1-\Omega)}{\Omega}$ is reduced which makes $S_i < 0$ in (41) a more restrict condition to satisfy.

C. Parameter synthesis: in the presence of deception attack

Theorem 3. Design observer gains L_i such that $A_{L_i} = A_i - L_i C_i$ is stable for $(1 \le i \le r)$. Tune the damping rate ζ_1, sampling period h, and attack parameters $\bar{\gamma}$ and $\bar{u}_s$ as initial parameters. If there exist the set of decision variables given in Theorem 1 (i.e., P_1, P_2, P_3, W, M, N, G, X_i) such that the following LMIs are satisfied

$$Y_{ii} < 0, \quad i = 1, \dots, r \tag{59}$$

$$\frac{2}{r-1} Y_{ii} + Y_{ij} + Y_{ji} < 0, \quad 1 \le i \ne j \le r \tag{60}$$

$$F_{ii} < 0, \quad i = 1, \dots, r \tag{61}$$

$$\frac{2}{r-1} F_{ii} + F_{ij} + F_{ji} < 0, \quad 1 \le i \ne j \le r \tag{62}$$

then the following control gains make system (21) stable

$$K_i = X_i (G^{-1})^T, \qquad (1 \le i \le r). \tag{63}$$

Undefined parameters are given below

$$Y_{ij} = \begin{bmatrix} S_{ij} & \Pi_{12,ij} \\ * & -\Pi_{22} \end{bmatrix}, \; F_{ij} = \begin{bmatrix} \Theta_{ij,1} + \Theta_2 & \Pi_{12,ij} & \Pi_{13} \\ * & -\Pi_{22} & 0 \\ * & * & -\Pi_{33} \end{bmatrix},$$

where S_{ij}, Θ_{ij}, and Θ_2 are previously defined in Theorem 1, and

$$\Pi_{12,ij} = \begin{bmatrix} B_i & B_i & B_i & 0 & 0 \\ B_i & B_i & B_i & \bar{\gamma} X_j^T & 0 \\ 0 & 0 & 0 & 0 & 0 \\ B_i & B_i & B_i & 0 & 0 \\ 0 & 0 & 0 & 0 & \bar{\gamma} X_j^T \end{bmatrix}, \; \Pi_{13} = \sqrt{\alpha h} \begin{bmatrix} M^T & hN^T \end{bmatrix},$$

$$\Pi_{22} = \text{diag}(I_m, I_m, I_m, I_m, I_m), \quad \Pi_{33} = \text{diag}(P_3, 3P_3).$$

Proof. We consider the same LLF given in (29) and expressions (30), (31), (32). Instead of (33), now the following null expression holds from the closed-loop system (21)

$$2\Big(\boldsymbol{x}^T(t) + \dot{\boldsymbol{x}}^T(t) + \boldsymbol{x}^T(t_k) \Big) G^{-1} \Big(- \dot{\boldsymbol{x}}(t)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3159582, IEEE Transactions on Smart Grid

$$+\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i\mu_j\Big\{A_i\boldsymbol{x}(t)+B_iK_j(\boldsymbol{x}(t_k)+\boldsymbol{e}(t_k))\Big\}$$
$$+\sum_{i=1}^{r}\mu_iB_i\left(\boldsymbol{\eta}_1(t)+\boldsymbol{\eta}_2(t)+\boldsymbol{u}_s(t_k)\right)\Big)=0, \quad (64)$$

where $\boldsymbol{\eta}_1(t) = \Gamma(t)\sum_{j=1}^{r}\mu_jK_j\boldsymbol{x}(t_k)$ and $\boldsymbol{\eta}_2(t) = \Gamma(t)\sum_{j=1}^{r}\mu_jK_j\boldsymbol{e}(t_k)$. From (14) it holds that

$$\boldsymbol{\eta}_1^T(t)\boldsymbol{\eta}_1(t)\leq\bar{\gamma}^2\boldsymbol{x}^T(t_k)\Big(\sum_{j=1}^{r}\mu_jK_j\Big)^T\Big(\sum_{j=1}^{r}\mu_jK_j\Big)\boldsymbol{x}(t_k), \quad (65)$$

$$\boldsymbol{\eta}_2^T(t)\boldsymbol{\eta}_2(t)\leq\bar{\gamma}^2\boldsymbol{e}^T(t_k)\Big(\sum_{j=1}^{r}\mu_jK_j\Big)^T\Big(\sum_{j=1}^{r}\mu_jK_j\Big)\boldsymbol{e}(t_k), \quad (66)$$

$$\boldsymbol{u}_s^T(t)\boldsymbol{u}_s(t)\leq\bar{u}_s^2. \quad (67)$$

Then, the proof mainly follows the same steps presented in Theorem 1. More precisely, by defining $\boldsymbol{\phi}_4=[\boldsymbol{\phi}_2,\boldsymbol{\eta}_1^T(t),\boldsymbol{\eta}_2^T(t),\boldsymbol{u}_s^T(t)]^T$ (where $\boldsymbol{\phi}_2$ is defined below (29)) the proof evolves to similar steps to (35)-(38). The Shure complement Lemma is used to include inequalities (65) and (66) in the LMI formulation. Considering $\bar{u}_s$ as the steady state (non-vanishing) error from the origin, it can be shown that if LMIs (59)-(62) are satisfied then the following condition is satisfied for $t\in[t_k,t_{k+1})$

$$\dot{V}(t)<-2\zeta_1V(t)+\bar{u}_s^2+\boldsymbol{b}^T(t_k)\bar{W}\boldsymbol{b}(t_k). \quad (68)$$

As mentioned previously, observer gains L_i are designed in such a way that $A_{L_i}=A_i-L_iC$ remains Hurwitz stable. Thus, $\boldsymbol{b}(t_k)$ asymptotically approaches zero. Therefore, condition (68) represents a bounded exponential stability for system (21) and this completes the proof. □

D. Parameter synthesis: co-existence of DoS and deception

Combining the set of LMI conditions given in Theorem 2 (parameter synthesis in the presence of DoS) and Theorem 3 (parameter synthesis in the presence of deception) leads to the following corollary for parameter synthesis for system (22) when DoS and deception attacks coexist.

Corollary 1. Design observer gains L_i such that $A_{L_i}=A_i-L_iC_i$ is Hurwitz stable for $(1\leq i\leq r)$. Tune ζ_1, h, $\Omega<1$, $\bar{\gamma}$, and $\bar{u}_s$ as initial parameters. If there exist the set of decision variables given in Theorem 1 (i.e., P_1, P_2, P_3, W, M, N, G, X_i) such that LMIs (43), (59), (60), (61), and (62) are satisfied then the control gains obtained from the same expression given in (63) make system (22) stable if the strength of DoS attacks satisfies (45).

Proof. Considering system (22), the proof follows the same steps given in Theorems 2 and 3. □

Remark 5. The scalability of the proposed approach can be discussed in two perspectives: (i) Scalability to the size of WP, and (ii) Scalability to the size of system matrix A in the controller design. The proposed approach is scalable to the WP size, as the WP is modeled using the 'aggregated turbine' technique [40], which simplifies the modeling procedure and is shown to be accurate enough for the SSI analysis [28]. Additionally, since the entire WP is modeled with a single turbine one can ensure that the size of matrix A remains the same. Only the entries of A may vary in response to the structural changes in the system (e.g., the number of WTs). From the control design perspective, since matrix A is directly used in the LMIs the computation complexity of solving the obtained LMIs inevitably depends on the size of A. This dependency on the size of A is common in related LMI-based works. As commented in Section V, through the hankle sigular value (HSV) technique one can reduce the size of A by preserving the modes with the highest amount of energy. In summary, the proposed approach is scalable from both perspectives.

TABLE I: The proposed methodology.

I. System modeling

I.1. Obtain the state space model (1) according to the operating point and fuzzy sets.

I.2. Reduce the model order based on the Hankel singular value (HSV) technique.

II. Parameter Design

II.1. Design observer gains L_i so that $A_{L_i}=A_i-L_iC_i$ is Hurwitz stable for $(1\leq i\leq r)$, where r is the number of fuzzy rules.

II.2. Select the desired values for the damping rate ζ_1, sampling period h, DoS resilience level Ω, deception parameters $\bar{\gamma}$, and $\bar{u}_s$.

II.3. Using a semi-definite programming software solve the following LMIs:
i) Attack free: Given $\{\zeta_1,h\}$ solve (24) to (27).
ii) DoS only: Given $\{\zeta_1,h,\Omega\}$ solve (39) to (43).
iii) Deception only: Given $\{\zeta_1,h,\bar{\gamma},\bar{u}_s\}$ solve (59) to (62).
iv) Both deception and DoS: Given $\{\zeta_1,h,\Omega,\bar{\gamma},\bar{u}_s\}$ solve (43), (59), (60), (61), and (62).

II.4. For a feasible solution of the LMIs solved in Step II.3, compute the required control gains using $K_i=X_i(G^{-1})^T$ for $(1\leq i\leq r)$.

Remark 6. The proposed secure sampled-data observer-based control for WP is summarized in Table I. Based on Table I, the proposed method can be categorized into two sections of 'system modeling' and 'parameter design'. In the system modeling section, first, the fuzzy state-space representation of the system is obtained and its order is reduced using the HSV technique. The use of HSV helps in reducing the the order of the WP which is usually significantly high. Then, the observer is designed in step II.1. Based on the under-study attack, steps II.2, II.3, and II.4 are followed to design the required resilient controller. Although the power system in this article is a WP with a complex stability issue, the proposed attack-resilient control scheme can be used in general cases where (i) the state space model of the system and its fuzzy sets are known, (ii) a central controller is used to maintain stability, and (iii) the adversary aims to execute one of the considered DoS and/or deception attacks. In other words, the system modeling section in Table I is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3159582, IEEE Transactions on Smart Grid

application-specific, i.e., the fuzzy linear state-space model and the system order after HSV reduction depends on the unique dynamics of the system under consideration. Once the model is determined, the parameter design stage can be applied to any system as a general procedure. That being said, the proposed method in this article can also be used for security control of a variety of other power system applications such as the load frequency control, wide-area and inter-area oscillation damping, and dynamic stabilization of DC microgrids.

Remark 7. From a security point of view, the considered DoS and deception attacks in this article cover a wide variety of common attacks on the controller $\boldsymbol{u}$ for different power applications. This includes the random DoS [23], periodic DoS [41], false data injection [17], and scaling attack on the controller [13] to name a few. It should be noted that, in another scenario, the attacker could block or manipulate the output measurements $\boldsymbol{y}$ (or system states $\boldsymbol{x}$) instead of the controller signal $\boldsymbol{u}$. For example, additive and scaling data integrity (DI) attacks on states have been studied for the load frequency control problem in [42]. In [43], the optimal load sharing is studied for cooperative microgrids, where the DI attack is considered for an internal localized state. Analogous to the problem formulation for deception attack in closed-loop system (21), the DI threats in outputs and states impose some disturbing terms in the closed-loop system. With some straightforward adjustments, Theorem 3 can be modified to cope with the DI attack on the state and output measurements. More precisely, one can modify variables $\boldsymbol{\eta}_1(t)$ and $\boldsymbol{\eta}_2(t)$ in (64) according to the impact of DI attack, and include new conditions in the form of (65)-(67) to develop sufficient LMI conditions. Therefore, the main benefits of the resilient design proposed in this article (i.e., the digital measurement, less conservative LLF-based stability analysis, and accommodating uncertainties in a fuzzy setting) is still applicable (with some modification) to such DI attacks on state and output measurements.

V. Simulations

This section conducts simulations to evaluate the performance of the proposed control schemes. The proposed LMIs are solved with the SDPT3 solver within the YALMIP parser. The time-domain simulations are performed using the EMTP-RV software, which simulates the detailed behavior of the power system [44]. The performance of the proposed control scheme is validated in Subsection V-E using a co-simulation framework. The detailed parameters of the WP are given in Table II.

The well-known grid-connected WP system, shown in Fig. 1, is used to test the performance of the proposed controller. The details of this system is given in [4]. Since the order of the open-loop system is high, the Hankel singular value (HSV) technique is used for model order reduction. The analysis of HSV, as shown in Fig. 6, demonstrates that a reduced order of $n = 7$ preserves most of the system

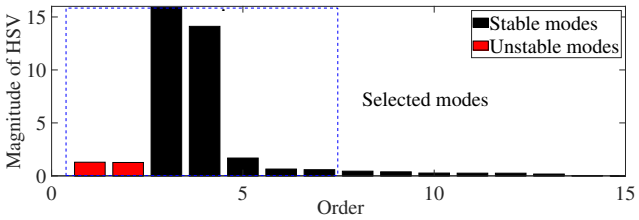

Fig. 6: Hankel singular values of the under-study system.

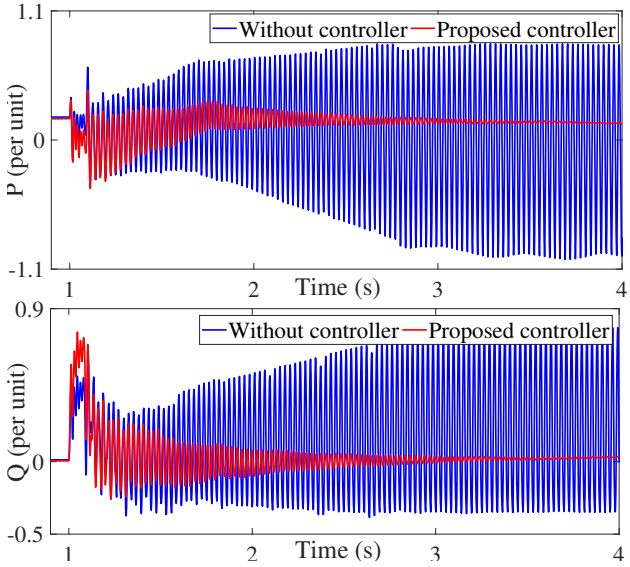

Fig. 7: Active and reactive power components of WP, i.e., P and Q, respectively, with and without the proposed controller.

characteristics (Steps I.1 and I.2 in Table I). The linearized model is represented by the following matrices

$$A=\begin{bmatrix} -0.008 & 1.40 & 0.89 & 0.69 & -0.37 & 0 & 0 \\ -1.35 & -52.24 & 1970.51 & -719.52 & -511.30 & 0 & 0 \\ -1.27 & -1978.50 & -57.49 & 620.29 & -676.55 & 0 & 0 \\ -0.25 & 765.70 & -567.45 & -91.98 & -2507.43 & 0 & 0 \\ 0.89 & 468.33 & 741.16 & 2528.38 & -93.83 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4.90 & -528.58 \\ 0 & 0 & 0 & 0 & 0 & 94.96 & 4.90 \end{bmatrix},$$

$$B^T=\begin{bmatrix} -0.02 & -1.44 & -2.32 & 3.86 & -2.22 & 0.74 & -1.07 \\ -0.07 & -1.99 & 1.88 & -1.86 & -3.72 & -3.05 & -0.47 \\ 0.12 & 1.88 & 8.96 & 1.60 & -10.65 & -3.49 & -1.80 \\ -0.03 & -8.49 & -0.19 & 10.47 & -0.52 & 3.27 & -1.22 \end{bmatrix},$$

$$C=\begin{bmatrix} -0.0009 & -3.4 & -6.94 & 9.15 & -6.0 & 0.16 & 9.04 \\ 0.03 & -6.58 & 4.90 & -5.64 & -9.32 & 5.44 & -0.49 \\ -0.02 & -2.23 & 3.49 & 1.37 & 2.52 & 0 & 0 \\ -0.14 & 4.60 & 2.20 & 3.63 & -1.69 & 0.0005 & -0.0014 \end{bmatrix}. \quad (69)$$

Since the states deployed in the full-state feedback controller are not physically meaningful (i.e., their measurement is not possible), an observer is designed using the LQR technique with $R = 6I$ and $Q = C^TC$. The designed observer gain is given below (Step II.1 in Table I)

$$L^T=\begin{bmatrix} -0.023 & 0.0017 & -0.0128 & 0.285 & 1.754 & -7.102 & 4.825 \\ -0.393 & -0.040 & 0.125 & -2.041 & 0.478 & 6.678 & 7.619 \\ 0.041 & 0.001 & 0.031 & -0.274 & -1.170 & 0.609 & -0.398 \\ 0.421 & 0.037 & -0.103 & 1.229 & -0.2447 & -0.218 & -0.687 \end{bmatrix}.$$

When a three-phase bolted fault occurs in Line A at t=1s, this line will be disconnected by the protection schemes using the CB2 and CB3 circuit breakers in 60ms and 80ms, respectively. The WP will be radially connected to a compensated line, and consequently the subsynchronous oscillations are initiated. Without any attack, the WP becomes unstable as shown in the blue waveforms of Fig. 7. Using model (69), the following control gain

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3159582, IEEE Transactions on Smart Grid

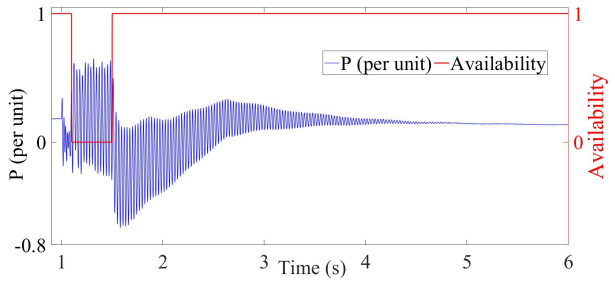

Fig. 8: Active power generation of the WP and availability of the designed controller in attack Sc.1.

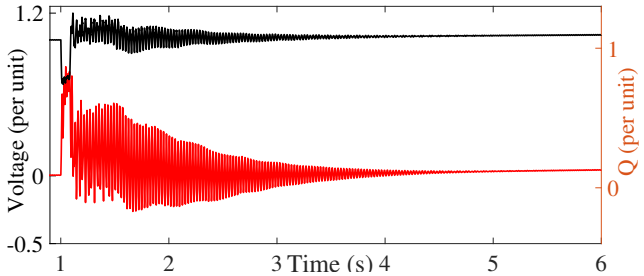

Fig. 9: The WP voltage and injected reactive power in Sc.1.

is designed from Theorem 1 with $\zeta_1 = 0.6$ and $h = 0.001s$ (based on Steps II.2-II.4 in Table I):

$$K = \begin{bmatrix} 2.21 & 0.0036 & 0.20 & 0.04 & 0.012 & 2.33 & 1.65 \\ 9.08 & 0.41 & 0.46 & 0.47 & -0.44 & 15.65 & -0.91 \\ -2.71 & -0.11 & -0.14 & -0.12 & 0.12 & -3.56 & 0.30 \\ -0.22 & 0.03 & -0.05 & -0.042 & -0.0006 & -0.84 & -0.22 \end{bmatrix}. \quad (70)$$

The red waveforms in Fig. 7 illustrate the ability of controller (70) to stabilize the system in almost 3s.

In the structure of the WT, the fault is detected by monitoring the voltage signal. An abrupt decrease in the voltage indicates the presence of a fault, and activates a fault-ride through (FRT) signal immediately. This FRT signal helps the turbine to generate enough reactive power for keeping the voltage as high as possible and wait for the protection systems to clear the short circuit if the fault prolongs. This FRT signal, which is also visible by the adversaries, indicates an SSI instability risk and informs them to initiate the attack. Even before the fault, the presence of adversary is stealthy from the WP operator since the SSI damping controller are often designed to respond when there is a disturbance in the system [28].

A. DoS attack

To inspect the performance of the controller during the attack, two different scenarios are considered: (i) **Sc.1** the adversary launches the attack in a single step, and (ii) **Sc.2** where the adversary uses a multi-step attack to target the system. It should be noted that the adversary is interested to destabilize the system with the minimum DoS attack to remain stealthy from the WP operator. From Theorem 2 with $h = 0.001$ and $\zeta_1 = 0.7$, we observer that the understudy system can tolerate up to 12% of DoS attack, i.e., a feasible controller can be computed from Theorem 2 with the maximum value for $\Omega = 0.12$. This gain is given below:

$$K = \begin{bmatrix} 3.48 & -0.03 & 0.15 & 0.07 & -0.03 & -0.11 & 12.24 \\ 6.38 & 0.11 & 0.13 & -0.04 & -0.09 & 4.38 & -0.84 \\ -4.20 & -0.048 & -0.10 & 0.009 & 0.061 & -0.63 & 1.22 \\ 0.68 & 0.05 & -0.02 & -0.05 & -0.012 & -0.36 & -2.04 \end{bmatrix}. \quad (71)$$

Fig. 8 demonstrates the active power generated by the WP and availability of the designed controller in Sc.1. The attack deteriorates the transient behavior of the system, but as expected, the controller is able to damp the oscillations. In order to show the impact of controller on the behavior of the WP, the voltage waveform and the injected reactive power are illustrated in Fig. 9. Both of the signals are within the acceptable range of operation.

In Sc.2, the adversary attacks in the following intervals.

$$D_0 = [1.1, 1.2), \quad D_1 = [1.5, 1.7), \quad D_2 = [1.8, 1.9). \quad (72)$$

With $\alpha_0 = 0.4$, $\alpha_1 = 9$, $\beta_0 = 1$, and $\beta_1 = 0.2$, condition (45) holds for attack sequence (72), i.e., $\frac{1}{9} + \frac{0.001}{0.2} < 0.12$. For this case, Figs. 10-11 show the active power injection, availability of the controller, and the reactive power and voltage of the WP, respectively. As shown, the proposed controller is still able to damp the oscillations.

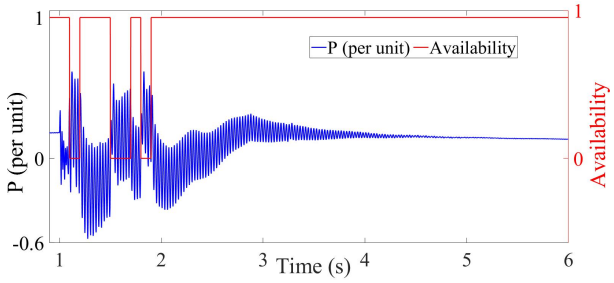

Fig. 10: Active power generation of the WP and availability of the designed controller in attack Sc.2.

B. Random DoS attack

This section studies the performance of the proposed controller designed using Theorem 2 against random DoS attacks. Let $T_f = 6$s denote the time horizon for simulation. We consider 4 attack intervals D_0 to D_3, where the start of each attack d_i $(0 \le i \le 3)$ and its duration τ_i $(0 \le i \le 3)$ follow a normal distribution $\mathcal{N}(\mu, \sigma^2)$.

TABLE II: System parameters

Parameter	Value	Parameter	Value	Parameter	Value	Parameter	Value
Nominal wind speed	11.24 m/s	$S_{WP-Trans}$	222 MVA	Length of Line A	100 km	Length of Line B	500 km
Q_{WP}^{nom}	0	$X_{WP-Trans}$	0.15 pu	R_{shunt}	10.8 Ω	X_{shunt}	1080 Ω
Number of WTs	133	$R_{WP-Trans}$	0.005 pu	R, system A	5 Ω	X, system A	75 Ω
P_{WT}	1.5 MW	$T_{rise-RSC}$	20 ms	R, system B	3.5 Ω	X, system B	75 Ω
S_{WT}	1.667 MVA	$T_{rise-GSC}$	10 ms	R Line	0.028 Ω/km	X Line	0.3244 Ω/km
V_{WT}	0.575 kV	K_v	2	C Line	5.0512 μS/km	$L_{mag-WT-Trans}$	2.9 pu
V_{MV}	34.5 kV	K_p	1	C_{MV}	23.5×10^{-6} F	WT pole pairs	3
V_{HV}	500 kV	$R_{stator-WT}$	0.033 pu	L_{MV}	12×10^{-5} H	L_{choke}	1.5 pu
R_{MV}	0.04 Ω	R_{choke}	0.015pu	$R_{WT-Trans}$	0.002 pu	$L_{rotor-WT}$	0.16 pu
$S_{WT-Trans}$	1.75 MVA	$R_{rotor-WT}$	0.026 pu	$X_{WT-Trans}$	0.06 pu	$L_{stator-WT}$	0.18 pu

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3159582, IEEE Transactions on Smart Grid

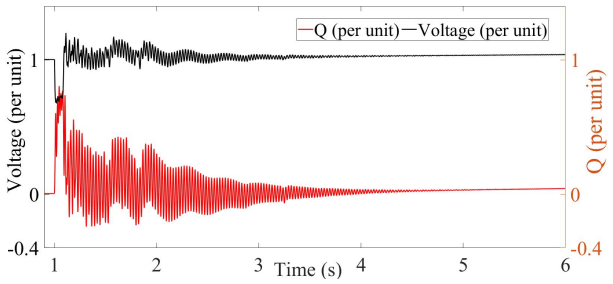

Fig. 11: The WP voltage and injected reactive power in Sc.2.

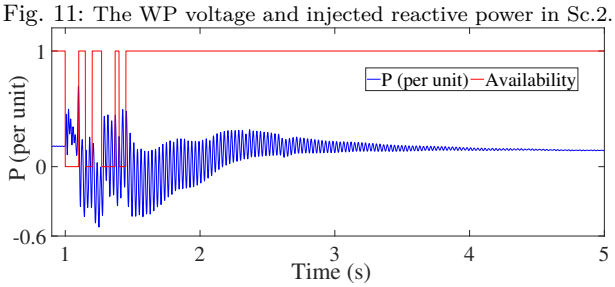

Fig. 12: Randomly generated DoS attack, Case I.

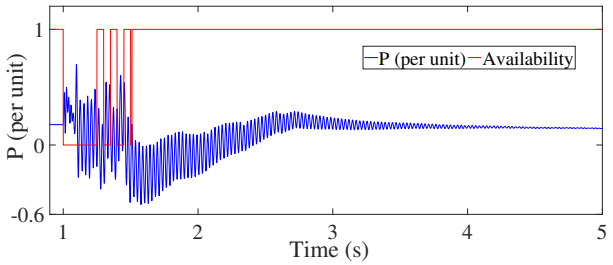

Fig. 13: Randomly generated DoS attack, Case II.

Let $\tau_i = |\omega_{1_i}|$, where $|\,.\,|$ is the absolute value of the argument and $\omega_{1_i} \sim \mathcal{N}(0.05, 0.1)$, $(0 \leq i \leq 3)$. Then, select $d_0 \sim \mathcal{N}(1, 0.5)$, (ignore the sign if negative), and

$$d_i = (d_{i-1} + \tau_{i-1}) + |\omega_{2_i}|, \quad i = 1, 2, 3,$$

with $\omega_{2_i} \sim \mathcal{N}(\frac{T_f - (d_{i-1}+\tau_{i-1})}{T_f - i}, 0.5)$. Only if the randomly generated DoS attacks D_0 to D_3 satisfy Assumption 1 with the given constants below expression (72), we run simulations. The resiliency of the WP system using controller (71) is evaluated under 100 randomly generated valid DoS sequences. We observe that the controller is able to damp the oscillations caused by the random attacks and the WP overall performance remains within the acceptable limits. For the sake of illustration, we have selected two of the worst-case simulated trajectories (named Case I and Case II) which are shown in Figs. 12 and 13.

C. Deception attack

Next, we study the resilience provided by Theorem 3 against deception attack on the controller. We consider the deception attack parameters as $\Gamma(t) = 0.15\sin(5t)I$, therefore it holds that $\bar{\gamma} = 0.15$. Fig. 14 shows the active power and voltage of the WP under the deception attack. The obtained controller from Theorem 3 is able to mitigate the SSI phenomenon without any sustained or growing oscillations in the WP parameters.

Now, we compare the result with [7]. Fig. 15 shows the active power generation of the system when the developed

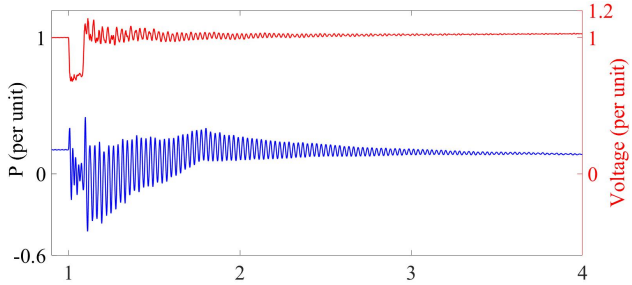

Fig. 14: Active power and voltage of the WP using Theorem 3 under deception attack.

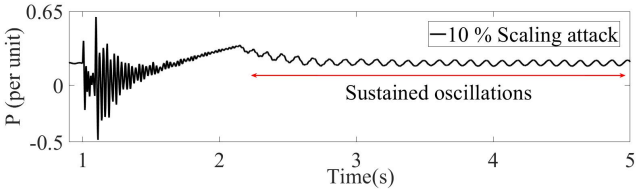

Fig. 15: The active power of controller developed in [7].

controller in [7] is implemented into the control loops and the adversary scales the control signals only 10%. It can be observed that despite the acceptable performance of the controller in damping the SSI phenomenon, there remains sustain oscillations in the WP behavior.

D. Coexistence of DoS and deception

Next, we consider that the WP is under both the deception and DoS attacks. To this end, we set $h = 0.001$s, $\zeta_1 = 0.7$, $\Omega = 0.07$ and $\bar{\gamma} = 0.05$ and obtain a controller from Corollary 1. It is observed that the computed controller is able to stabilize the WP system under the coexistence of both attacks. Note that the tolerable amount of attacks are smaller compared to the case of solitary DoS or solitary deception attacks. For example, with $\zeta_1 = 0.7$ and $h = 1$ms, the largest feasible values for DoS and deception are, respectively, $\Omega = 0.081$ and $\bar{\gamma} = 0.054$.

E. Fuzzy control

As discussed in Subsection II-C, the structure of a power system, e.g., the impedance of System B in Fig. 1, is uncertain. This impedance is used in our Fuzzy model since it has significant impact on the SSI severity and is also unknown to the WP operator. In the operation, the actual impedance from the WP point of view can be measured using available voltage and current measurements at POI ($Z_{grid} = V_{WF}/I_{LB}$, where V_{WF} and I_{LB} are the voltage of the WP terminal and current of Line B, respectively). This impedance along with the prior knowledge of the Line B impedance (Z_{LB}) gives the control scheme an estimation about the System B impedance, and consequently a parameter to determine the coefficients between a set of designed Fuzzy controllers as shown in Fig. 16.

In order to show the performance of the proposed Fuzzy scheme, three other scenarios are considered and simulated in a co-simulation platform shown in Fig. 17. In Sc.3, a 80% decrease occurs at t=1s in the impedance of the System B of the considered benchmark, where the system

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3159582, IEEE Transactions on Smart Grid

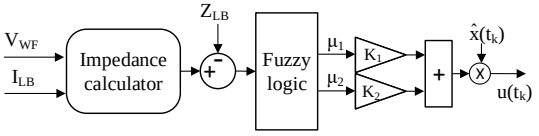

Fig. 16: The diagram of Fuzzy control scheme.

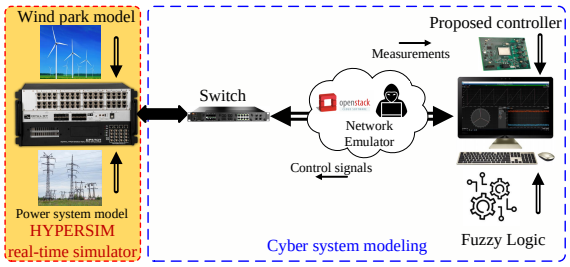

Fig. 17: The developed co-simulation platform.

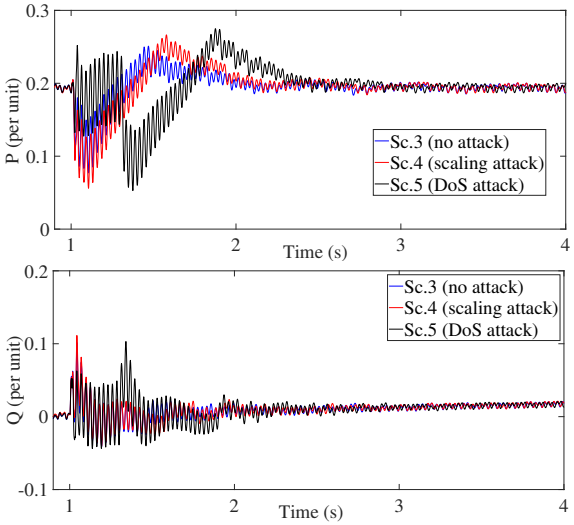

Fig. 18: Active and reactive power generation in Sc.3-5.

is on an attack-free state. In Sc.4, similar condition occurs in the grid and at the same time. An adversary launches a 15% deception attack. In Sc.5 and similar to the last two scenarios, following a decrease in the impedance of System B, the adversary also launches a DoS attack. The active and reactive power generation of the WP in Sc.3-5 are shown in Fig. 18. The Fuzzy logic for the controller is $K = 0.5(1+dm/dt)K_1 + 0.5(1-dm/dt)K_2$, where m is the estimated impedance of System B. Controllers K_1 and K_2 are also designed based on the 20% range of impedance variation, i.e., $Z_{min} = 80\%Z_{nom}$. It can be observed that the proposed controller is able to damp the oscillations and preserve the system stability in a satisfactory manner.

F. Comparison with [4] and [8]

We compare the performance of the controller designed from Theorem 2 (DoS resilient) with [4], where the μ-technique is used by considering the uncertainties of the WP parameters. Unlike Theorem 2, the impact of possible cyber attacks has been overlooked in [4]. Fig. 19 shows the performance of the two controllers when the wind speed is 0.7 pu. It is observed that both controllers provide almost similar behavior, while the damping of the designed controller from Theorem 2 is slightly slower compared to [4].

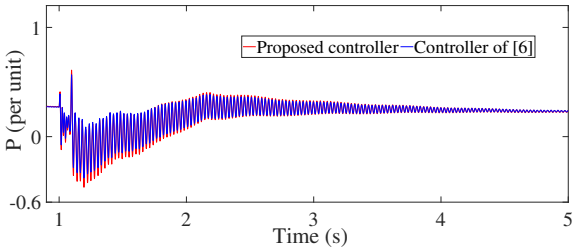

Fig. 19: Comparison between the performance of the designed controller in Theorem 2 and [4].

Similar to many other cyber-security improvements, the proposed method comes at the cost of a slightly reduced rate for damping. However, the performance is still within the acceptable level. Thus, the improved cyber-security of the controller overshadows the slight performance drop.

Next, we compare the largest allowable sampling period obtained from Theorem 1 in this article (attack-free situation) with that of [8, Theorem 1]. We remind that the stability conditions in [8] are obtained based on an LKF approach, while the method used in the present article is an LLF one. As mentioned in Remark 3, the LLF method is less conservative by nature. To numerically validate this fact, we set $\zeta_1 = 0.6$ and find the maximum allowable sampling periods provided by [8, Theorem 1] and Theorem 1 in this article. The maximum guaranteed sampling period by [8, Theorem 1] is obtained as $h_{M1} = 0.0012$. This value for Theorem 1 in this work is calculated as $h_{M2} = 0.0022$ which, as expected, is higher than h_{M1} and corroborates a less conservative control design.

VI. Conclusion

This article delivers the first SSI damping observer-based fuzzy controller with guaranteed level of resilience to denial of service (DoS) and deception attacks. The required conditions for designing the controller are developed based on a looped-Lyapunov functional technique. The use of sampled-data scheme makes our design suitable for digital implementation. Despite the fact that the cyber attacks on WPs are mostly overlooked in the literature, the developed controller guarantees a level of resiliency against the considered attacks. Moreover, the Fuzzy control scheme ensures a satisfactory performance in the presence of wind park uncertainties. Collected results from EMT simulations and a co-simulation framework verify the ability of the proposed controller in the presence of DoS and deception attacks. In future, we will study secure conditions against replay attacks on the WP system.

References

[1] A. Golshani, W. Sun, Q. Zhou, Q. P. Zheng, and Y. Hou, "Incorporating wind energy in power system restoration planning," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 16–28, 2017.

[2] "World adds record new renewable energy capacity in 2020," *International Renewable Energy Agency (IRENA)*, April. 2021.

[3] J. Bialek, "What does the power outage on 9 august 2019 tell us about GB power system," 2020, https://doi.org/10.17863/CAM.52486.

[4] M. Ghafouri, U. Karaagac, H. Karimi, S. Jensen, J. Mahseredjian, and S. O. Faried, "An LQR controller for damping of subsynchronous interaction in DFIG-based wind farms," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4934–4942, 2017.

[5] P. Huang, M. S. El Moursi, and et. al, "Subsynchronous resonance mitigation for series-compensated DFIG-based wind farm by using two-degree-of-freedom control strategy," *IEEE Trans. Power Syst.*, vol. 30, no. 3, pp. 1442–1454, 2015.

[6] X. Shi, Y. Cao, M. Shahidehpour, Y. Li, X. Wu, and Z. Li, "Data-driven wide-area model-free adaptive damping control with communication delays for wind farm," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5062–5071, 2020.

[7] M. Ghafouri, U. Karaagac, H. Karimi, and J. Mahseredjian, "Robust subsynchronous interaction damping controller for DFIG-based wind farms," *J. Mod. Power Syst. Clean Energy*, vol. 7, no. 6, pp. 1663–1674, 2019.

[8] A. Amini, A. Asif, A. Mohammadi, and A. Azarbahram, "Sampled-data dynamic event-triggering control for networked systems subject to dos attacks," *IEEE Trans. Netw. Sci. Eng.*, early access, 2021, doi: 10.1109/TNSE.2021.3070804.

[9] R. Venkateswaran and Y. H. Joo, "Retarded sampled-data control design for interconnected power system with DFIG-based wind farm: LMI approach," *IEEE Trans. Cybern.*, 2021, early access, doi: 10.1109/TCYB.2020.3042543.

[10] H.-B. Zeng, K. L. Teo, and Y. He, "A new looped-functional for stability analysis of sampled-data systems," *Automatica*, vol. 82, pp. 328–331, 2017.

[11] G. Chen, J. Xia, J. H. Park, H. Shen, and G. Zhuang, "Sampled-data synchronization of stochastic markovian jump neural networks with time-varying delay," *IEEE Trans. Neural Netw. Learn.*, early access, 2021, doi: 10.1109/TNNLS.2021.3054615.

[12] L. Pan and X. Wang, "Variable pitch control on direct-driven PMSG for offshore wind turbine using repetitive-TS fuzzy PID control," *Renewable Energy*, vol. 159, pp. 221–237, 2020.

[13] M. Ghafouri, U. Karaagac, A. Ameli, J. Yan, and C. Assi, "A cyber attack mitigation scheme for series compensated DFIG-based wind parks," *IEEE Trans. on Smart Grid*, early access, 2021, doi: 10.1109/TSG.2021.3091535.

[14] J. Yan, C. Liu, and M. Govindarasu, "Cyber intrusion of wind farm scada system and its impact analysis," in *2011 IEEE/PES Power Systems Conference and Exposition*, 2011, pp. 1–6.

[15] "*Roadmap for Wind Cybersecurity*. Accessed: Jul. 2020. [online]. Available: https://www.osti.gov/biblio/1647705."

[16] Z. Lian, F. Guo, C. Wen, C. Deng, and P. Lin, "Distributed resilient optimal current sharing control for an islanded DC microgrid under DoS attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4494 – 4505, 2021.

[17] M. Li and Y. Chen, "Wide-area robust sliding mode controller for power systems with false data injection attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 922–930, 2019.

[18] Y.-L. Huang, A. A. Cardenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 2, no. 3, pp. 73–83, 2009.

[19] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber–physical systems," *ISA trans.*, early access, 2021, doi: 10.1016/j.isatra.2021.01.036.

[20] L. An and G.-H. Yang, "Improved adaptive resilient control against sensor and actuator attacks," *Inf. Sci.*, vol. 423, pp. 145–156, 2018.

[21] Y. Yang, Y. Li, D. Yue, Y.-C. Tian, and X. Ding, "Distributed secure consensus control with event-triggering for multiagent systems under DoS attacks," *IEEE Trans. Cybern.*, vol. 51, no. 6, pp. 2916–2928, 2020.

[22] C.-H. Xie and G.-H. Yang, "Observer-based attack-resilient control for linear systems against FDI attacks on communication links from controller to actuators," *Int. J. Robust Nonlin.*, vol. 28, no. 15, pp. 4382–4403, 2018.

[23] Z. Hu, S. Liu, W. Luo, and L. Wu, "Resilient distributed fuzzy load frequency regulation for power systems under cross-layer random denial-of-service attacks," *IEEE Trans. Cybern.*, 2020, early access, doi: 10.1109/TCYB.2020.3005283.

[24] E. Tian and C. Peng, "Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks," *IEEE Trans. Cybern.*, vol. 50, no. 11, pp. 4610–4618, 2020.

[25] D. Zhao, Z. Wang, G. Wei, and Q.-L. Han, "A dynamic event-triggered approach to observer-based PID security control subject to deception attacks," *Automatica*, vol. 120, p. 109128, 2020.

[26] Y. Zhang, Y. Xiang, and L. Wang, "Power system reliability assessment incorporating cyber attacks against wind farm energy management systems," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2343–2357, 2017.

[27] A. E. Leon, S. Amodeo, and J. M. Mauricio, "Enhanced compensation filter to mitigate subsynchronous oscillations in series-compensated DFIG-based wind farms," *IEEE Trans. Power Deliv.*, early access, 2021, doi: 10.1109/TPWRD.2021.3049318.

[28] M. Ghafouri, U. Karaagac, J. Mahseredjian, and H. Karimi, "SSCI damping controller design for series-compensated DFIG-based wind parks considering implementation challenges," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 2644–2653, 2019.

[29] U. Karaagac, S. O. Faried, J. Mahseredjian, and A.-A. Edris, "Coordinated control of wind energy conversion systems for mitigating subsynchronous interaction in DFIG-based wind farms," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2440–2449, 2014.

[30] S. V. Bozhko, R. Blasco-Gimenez, R. Li, J. C. Clare, and G. M. Asher, "Control of offshore DFIG-based wind farm grid with line-commutated hvdc connection," *IEEE Transactions on Energy Conversion*, vol. 22, no. 1, pp. 71–78, 2007.

[31] A. Yogarathinam and N. R. Chaudhuri, "Wide-area damping control using multiple DFIG-based wind farms under stochastic data packet dropouts," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3383–3393, 2018.

[32] M. A. Ahmed, A. M. Eltamaly, M. A. Alotaibi, A. I. Alolah, and Y.-C. Kim, "Wireless network architecture for cyber physical wind energy system," *IEEE Access*, vol. 8, pp. 40 180–40 197, 2020.

[33] S. Hara, Y. Yamamoto, and H. Fujioka, "Modern and classical analysis/synthesis methods in sampled-data control-A brief overview with numerical examples," *Proc. IEEE Conf. Decis. Control*, vol. 2, pp. 1251–1256, 1996.

[34] V. Phat, Y. Khongtham, and K. Ratchagit, "LMI approach to exponential stability of linear systems with interval time-varying delays," *Linear Algebra Appl.*, vol. 436, no. 1, pp. 243–251, 2012.

[35] C. De Persis, P. Tesi *et al.*, "Input-to-state stabilizing control under denial-of-service." *IEEE Trans. Automat. Contr.*, vol. 60, no. 11, pp. 2930–2944, 2015.

[36] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Trans. Cybern.*, vol. 49, no. 99, pp. 1–11, 2018.

[37] H.-B. Zeng, K. L. Teo, Y. He, H. Xu, and W. Wang, "Sampled-data synchronization control for chaotic neural networks subject to actuator saturation," *Neurocomputing*, vol. 260, pp. 25–31, 2017.

[38] P. Park, J. W. Ko, and C. Jeong, "Reciprocally convex approach to stability of systems with time-varying delays," *Automatica*, vol. 47, no. 1, pp. 235–238, 2011.

[39] H. D. Tuan, P. Apkarian, T. Narikiyo, and Y. Yamamoto, "Parameterized linear matrix inequality techniques in fuzzy control system design," *IEEE Trans. Fuzzy Syst.*, vol. 9, no. 2, pp. 324–332, 2001.

[40] E. Muljadi, C. Butterfield, A. Ellis, J. Mechenbier, J. Hochheimer, R. Young, N. Miller, R. Delmerico, R. Zavadil, and J. Smith, "Equivalencing the collector system of a large wind power plant," in *2006 IEEE Power Engineering Society General Meeting*, 2006.

[41] P. Chen, D. Zhang, L. Yu, and H. Yan, "Dynamic event-triggered output feedback control for load frequency control in power systems with multiple cyber attacks," *IEEE Trans. Syst. Man Cybern.: Syst.*, early access, 2022, doi: 10.1109/TSMC.2022.3143903.

[42] H. Yang, S. Liu, and C. Fang, "Model-based secure load frequency control of smart grids against data integrity attack," *IEEE Access*, vol. 8, pp. 159 672–159 682, 2020.

[43] S. Sahoo and J. C.-H. Peng, "A localized event-driven resilient mechanism for cooperative microgrid against data integrity attacks," *IEEE Trans. on Cybern.*, vol. 51, no. 7, pp. 3687–3698, 2020.

[44] J. Mahseredjian, S. Dennetière, L. Dubé, B. Khodabakhchian, and L. Gérin-Lajoie, "On a new approach for the simulation of transients in power systems," *Electric Power Systems Research*, vol. 77, no. 11, pp. 1514–1520, 2007.