Wide-Area Damping Control Resilience towards Cyber-Attacks
A Dynamic Loop Approach

Patel, Abhilash; Roy, Spandan; Baldi, Simone

DOI
10.1109/TSG.2021.3055222

Publication date
2021

Document Version
Accepted author manuscript

Published in
IEEE Transactions on Smart Grid

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.2021.3055222, IEEE Transactions on Smart Grid

Wide-Area Damping Control Resilience towards Cyber-Attacks: A Dynamic Loop Approach

Abhilash Patel, Spandan Roy, and Simone Baldi

***Abstract*—By increasingly relying on network-based operation for control, monitoring, and protection functionalities, modern wide-area power systems have also become vulnerable to cyber-attacks aiming to damage system performance and/or stability. Resilience in state-of-the-art methods mostly relies on known characteristics of the attacks and static control loops (i.e., with fixed input/output channels). This work proposes a 'dynamic loop' wide-area damping strategy, where input/output channel pairs are changed dynamically. We study 'reactive' dynamic switching in case of detectable attack and 'pro-active' dynamical switching, in case of undetectable (stealth) attacks. Stability of the dynamic loop is presented via Lyapunov theory, under parametric perturbations, average dwell time switching and external perturbations. Using two- and five-area IEEE benchmarks, it is shown that the proposed strategy provides effective damping and robustness under various detectable (e.g., false data injection, denial-of-service) and stealth (replay, bias injection) attacks.**

***Index Terms*—Cyber-attack, Dynamic Loop, Resilience, Switched Controller, Wide-Area Damping Control.**

I. Introduction

Oscillations in power systems can limit the achievable performance of the grid, and may hamper its stability. With advances in smart grid equipped with non-inertial sources, the threat of oscillations is more and more serious [1], [2]. Among the different types of oscillations, swing modes play a crucial role. The presence of swing modes poses a limit to the power transfer capability. Based on their participation, swing modes can be categorized as local modes and inter-area modes. In local modes, synchronous machines in one area oscillate against the synchronous machines from the same area; in inter-area modes, synchronous machines from one area oscillate against synchronous machines from another area connected through a tie-line [3]. In general, the local modes can be damped using a local power system stabilizer (PSS) with feedback from local measurements. However, inter-area modes are less observable from local measurements: therefore, a combination of remote and local signals is used as feedback, resulting in a wide-area damping controller (WADC) [4].

Remote signals are readily available nowadays due to deployment of Phasor Measurement Unit (PMU) connected to a wide-area measurement system [5]. A PMU can transmit the signal to controller through phasor data concentrator using communication channels. These measurements are used for control, monitor and protection purposes [6] (cf. Fig. 1). However, by sharing information through a communication network, WADC becomes vulnerable to cyber-attacks in communication channels [7]–[13]. It has been noted that such attacks lead to degraded performances, cascaded failures and even loss of stability. One famous example is the 2015 Ukarine's power system outage due to a cyber-attack which affected more than 20000 customers [14].

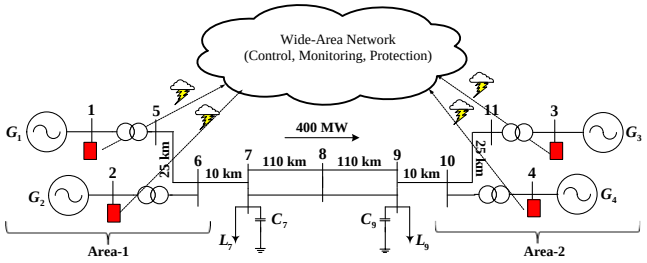


Figure 1. Network representation of wide-area damping controller: signals used for control can be compromised by malicious attacks.

As cyber-attacks can be a serious threat to system operation, numerous approaches have been developed to provide grid resilience. For example, WADC can be augmented with cyphered communication protocols [15], [16], with observers aiming to detect an attack and initiate necessary protective actions [17]–[19], or can be designed with the objective of achieving robustness against specific attacks in WADC [20]–[28] and load frequency control [29], [30] settings. However, these approaches are effective only for specific types of attacks, as explained in the following motivating example.

A. Motivation for This Work

Using a power systems benchmark, let us illustrate the motivations for the need of a novel framework to grid resilience.

Benchmark example: The benchmark two-area system [31] consists of 11 buses and 4 generators (denoted as G_i) as shown in Fig. 1. Each area is equipped with a local PSS to provide damping of local modes. Measurements for inter-area damping can be selected based on the loop selection index (LSI), which quantifies controllability and observability[1]

The first two authors equally contributed to the work. This work was partially supported by Seed Grant IIIT/19-20/003 India, by Special Guiding Funds Double First-class grant 3307012001A, and by Natural Science Foundation of China grant 62073074 (corresponding author: S. Baldi).

A. Patel is with Electrical Engineering Department, Indian Institute of Technology Delhi (IIT Delhi), Delhi, India e-mail: abhilash.patel@ee.iitd.ac.in
S. Roy is with Robotics Research Centre, International Institute of Information Technology Hyderabad (IIIT-H), India e-mail: spandan.roy@iiit.ac.in
S. Baldi is with School of Mathematics, Southeast University, Nanjing, China, and guest with Delft Center for System and Control, Delft University of Technology (TU Delft), The Netherlands e-mail: s.baldi@tudelft.nl

[1]Other popular indices are the approximate decentralized fixed mode [32] and the singular values [33].

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.2021.3055222, IEEE Transactions on Smart Grid

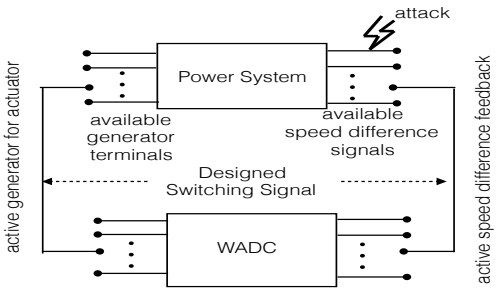


Figure 2. Block diagram for dynamic loop strategy that can enhance the grid resiliency to attack.

corresponding to the inter-area mode [34]. For the benchmark two-area system (Fig. 1), the LSI results in selecting $\Delta\omega_{(2,4)}$ (speed deviation between G_2 and G_4) as feedback signal and G_4 as actuation node [31], [35]. Speed deviations are used as feedback signals, since they have been proven to be strongly correlated with inter-area modes [4]. In this scenario, WADC is a 'static loop' meaning that the feedback loop is fixed by the '(feedback signal, actuation node)' pair. However, such static loop becomes vulnerable to cyber-attacks if an adversary gains the knowledge of which measurement and actuation nodes are used in the WADC loop. For example:

Reactive scenario: In presence of cyber attacks, data may be compromised at both input and/or output channels (e.g. false data injection, denial-of-service) and can no longer be used directly to the controller. One approach to solve such issue is to consider alternative '(feedback signal, actuation node)' pairs: such situation is accordingly termed *reactive* as measures are taken a posteriori to detecting an attack.

Proactive scenario: However, sometimes it becomes difficult to detect an attack, e.g., if it is of stealth nature such as replay attack or bias injection attack [36]. Under such circumstances, *reactive measures are ineffective*. An effective solution, as investigated in this work, can be to *pro-actively switch* among different loops. For example, in the two area system in Fig. 1, the designer can dynamically switch to alternative '(feedback signal, actuation node)' pairs, such as ($\Delta\omega_{(2,4)}$, G_4), ($\Delta\omega_{(1,4)}$, G_3), ($\Delta\omega_{(2,3)}$, G_1) etc. to evade possible stealth attacks.

Both the reactive and the pro-active scenarios highlight the limitation of static control loops and motivate the quest for a 'dynamic WADC loop' strategy to grid resilience (cf. Fig. 2). In the following, in order to keep the presentation simple and closer to the dynamic loop strategy idea, we will avoid introducing further complications such as false alarms in attack detection or failures in the physical infrastructure.

B. Contributions

In this paper, a switched wide-area damping controller is designed based on 'dynamic loop' idea. The contributions are:

- Resilience is designed without relying on the nature of the attack: the design philosophy is to guarantee stable operation despite dynamical changes in the control topology. In both the reactive and the pro-active scenario, dynamical switching still maintains system stability.
- Closed-loop stability of the dynamic loop strategy is analytically derived, in the presence of system parametric uncertainty, average dwell time (ADT) switching and external disturbances. ADT switching provides the flexibility to deal with unknown occurrence of detectable attacks or stealth attacks (cf. Remark 1 for details).
- The effectiveness of the proposed dynamic loop strategy is demonstrated via the IEEE benchmarks under various reactive (detectable attacks) and pro-active (stealth attacks) scenarios. It is shown that attacking a static loop WADC not only can deteriorate the system performance but may also cause instability; whereas, the proposed WADC can damp the oscillation in all attack scenarios.

It is worth mentioning that, when selecting multiple (feedback signals, actuation node) pairs for WADC, the optimality may be sacrificed in favour of increased robustness against attacks. For example, if optimal performance is quantified in terms of LSI (controllability and observability index), one has that if the best controllable and observable pair is subject to attack, it is necessary to switch to a different pair with a lower LSI index. The optimality/robustness trade-off is well known in cyber-security literature [37].

The rest of the paper is organized as follows: Section II formulates the control problem; The proposed dynamic loop controller is in Section III; Sections IV and V presents the comparative simulation results using the IEEE benchmarks and concluding remarks are in Section VI.

II. SYSTEM DESCRIPTION AND PROBLEM FORMULATION

Although wide-area power systems are inherently nonlinear, the IEEE Task Force Report on Benchmark System [39] has provided guidelines for obtaining small-signal linearised models for control design. This leads to linear dynamics standardly adopted in wide-area control literature (cf. [7]–[10], [17]–[28] and references therein). The model of a power system with 'm' synchronous generators results in

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B_i u_i(t) \\ y_{ij}(t) &= C_{ij} x(t) \end{aligned} \tag{1}$$

where $i = \{1, 2, \ldots, m\}$, $x \in \mathbb{R}^n$ are the states of the power system (e.g. load angle, speed deviation, exciter voltages); u_i is the control signal to the generator excitation system of the i^{th} synchronous machine; y_{ij} is the speed difference between a local i^{th} synchronous machine and a remote j^{th} machine from another area; A is the system state matrix; B_i and C_{ij} are input and output vectors of adequate dimension. Indices such as LSI determine the '(feedback signal, actuation node)' pair, and thus triplet $\{A, B_i, C_{ij}\}$ (cf. Tables I and II in the simulation sections). One might argue if using other feedback signals than speed deviation might improve resilience. Unfortunately, this is not suggested since measuring these signals require installation of extra sensors (while the speed deviation measurement is available from installed PMUs, cf. [4]–[7]); having extra sensors will also require extra communication, which can increase vulnerability.

To provide grid resilience against a cyber-attack, we look for enhancing WADC with a 'dynamic loop'. Such a loop can

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.2021.3055222, IEEE Transactions on Smart Grid

be represented by a switching signal, i.e., by mapping B_i and C_{ij} into $B_\sigma \in \mathcal{B}$ and $C_\sigma \in \mathcal{C}$ where $\sigma(t)$ is the switching signal, $\sigma(t) : [0\ \infty) \mapsto \Omega$ taking values in $\Omega = 1, 2, \ldots, N$, where N is the cardinality of a set for the permutation of i^{th} machine for actuation and $i^{th} - j^{th},\ i \neq j$ and i and j is from different area wide-area measurements. A representative example is depicted in Fig. 3. Here, t_k defines the instances (i.e. '*when*') of switching: in case of 'reactive' scenario, t_k is determined by the detection of an attack, and in case of 'pro-active' scenario t_k is 'designed' by the user to avoid possible attacks. On the other hand, $\sigma(\cdot)$ defines *'where'* to switch in the either of reactive of pro-active scenario: that is, $\sigma(\cdot)$ determines the 'next' combination of (B_σ, C_σ) to be activated: note that in the pro-active scenario $\sigma(t_k)$ might be known in advance, whereas in the reactive one it is typically unknown a priori. The time $t \in [t_k\ \ t_{k+1})$ between consecutive switching instants is called the 'dwell-time' and its value should be properly designed in order to guarantee stability of the dynamic loop [38].

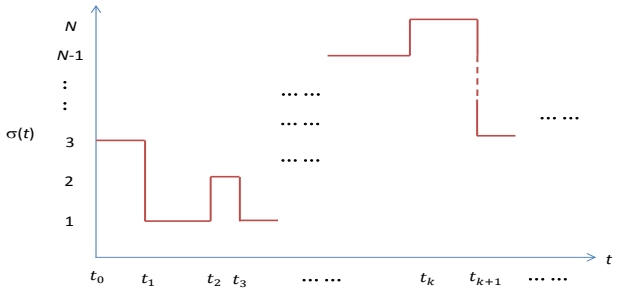


Figure 3. A representative switching signal σ

Definition 1: Average Dwell Time (ADT) [38]: For a switching signal $\sigma(\cdot)$ and each $t_2 \geq t_1 \geq 0$, let $N_\sigma(t_1, t_2)$ denote the number of discontinuities in the interval $[t_1, t_2)$. Then $\sigma(\cdot)$ has an average dwell time ϑ if

$$N_\sigma(t_1, t_2) \leq N_0 + (t_2 - t_1)/\vartheta, \quad \forall t_2 \geq t_1 \geq 0, \tag{2}$$

where the scalar $N_0 > 0$ is termed as chatter bound.

Remark 1 (Significance of ADT): The notion of ADT in (2) signifies that a short dwell-time $(t_{k+1} - t_k) < \vartheta$ must be compensated by a larger dwell-time, i.e., $(t_{k+1} - t_k) > \vartheta$ at later stage: in other words, the dwell time is defined in an average sense. The adoption of ADT has some specific design advantages: (i) in reactive scenario, one cannot determine a priori when an attack might occur. If such situation is detected before the stipulated dwell-time (i.e., $(t_{k+1} - t_k) < \vartheta$) then it can be compensated later by a larger dwell time; (ii) in a pro-active scenario, a designer can suitably shorten and lengthen the dwell-time so that a potential attack can be avoided.

After incorporating the switching signal, as well as the inevitable uncertainty in power system parameters, the model described in (1) can be compactly represented as,

$$\dot{x}(t) = A_p x(t) + B_{p\sigma(t)} u_{p\sigma(t)}(t) + W(t) \tag{3a}$$

$$y_{\sigma(t)}(t) = C_{\sigma(t)} x(t) \tag{3b}$$

where $A_p(t) = A + \Delta A(t)$ and $B_{p\sigma(t)}(t) = B_{\sigma(t)} + \Delta B_{\sigma(t)}(t)$, respectively. The terms $A, B_{\sigma(t)}$ denote known nominal values, while $\Delta A(t), \Delta B_{\sigma(t)}(t)$ represent bounded parametric perturbations and $W(t)$ is a bounded exogenous signal. The following assumption outlines the nature of uncertainties:

Assumption 1 (Uncertainty): The perturbation values $\Delta A(t), \Delta B_\sigma(t)$ are not known instantaneously; but there exist known scalars $\delta a, \delta b \in \mathbb{R}^+$ such that $||\Delta A(t)|| \leq \delta a$ and $||\Delta B_\sigma(t)|| \leq \delta b\ \forall t$. Further, $W(t)$ is unknown but bounded as $||W(t)|| \leq \bar{w}$ where $\bar{w}$ is unknown.

Assumption 2: The dimension of the state n remains constant during WADC operation.

Remark 2: Assumption 1 requires a robust design, i.e., a stable controller under worst case uncertainty in line with [20]–[24]. Assumption 2 implies that no area becomes isolated. Violation of Assumption 2 leads to impulse behaviour that can be possibly handled by the proposed approach, but proving its formal stability requires ad-hoc analysis which can be the subject of future work.

Switched WADC Problem: For the wide area power system (3), the control problem is to design a robust dynamic WADC loop that guarantees stable operation in the presence of uncertainties as in Assumption 1, with switching signals as in Definition 1, and under reactive and pro-active scenarios.

III. Control Design and Analysis

From now on, let us drop for compactness the time index t whenever unambiguous. A dynamic output feedback switched WADC is proposed as

$$\begin{aligned} \dot{x}_c &= E_\sigma x_c + F_\sigma y, \\ u_\sigma &= L_\sigma x_c, \end{aligned} \tag{4}$$

where E_σ, F_σ and L_σ are user-defined constant matrices and their design will be detailed later in this section. Notice that the presence of the index σ implies that the control also switches with the system. Substituting (4) into (3) the closed-loop dynamics is obtained as follows:

$$\begin{aligned} \dot{x} &= (A + \Delta A)x + (B_\sigma + \Delta B_\sigma) L_\sigma x_c + W, \\ \dot{x}_c &= E_\sigma x_c + F_\sigma C_\sigma x. \end{aligned}$$

Defining $\chi \triangleq [x^T\ \ x_c^T]^T$, the closed-loop dynamics can be compactly represented as

$$\dot{\chi} = (\overline{A}_\sigma + \Delta\overline{A}_\sigma)\chi + \overline{W}, \tag{5}$$

where

$$\overline{A}_\sigma = \begin{bmatrix} A & B_\sigma L_\sigma \\ F_\sigma C_\sigma & E_\sigma \end{bmatrix}, \Delta\overline{A}_\sigma = \begin{bmatrix} \Delta A & \Delta B_\sigma L_\sigma \\ 0 & 0 \end{bmatrix}, \overline{W} = \begin{bmatrix} W \\ 0 \end{bmatrix}.$$

Let the matrices E_σ, F_σ and L_σ be designed in a way such that the following Lyapunov condition is satisfied:

$$\overline{A}_\sigma^T P_\sigma + P_\sigma \overline{A}_\sigma < -\alpha_\sigma P_\sigma \quad \forall \sigma \in \Omega, \tag{6a}$$

$$\iota_\sigma \triangleq [\alpha_\sigma \lambda_{\min}(P_\sigma) - 2||P_\sigma||\zeta_\sigma] > 0, \quad \forall \sigma \in \Omega. \tag{6b}$$

$$\zeta_\sigma \geq ||\Delta\overline{A}_\sigma(t)||\ \forall t, \tag{6c}$$

where α_σ is a positive user-defined scalar; ζ_σ in (6c) can be determined from the knowledge of the uncertainty upper bounds δa and δb (cf. Assumption 1) and via the structure of $\Delta\overline{A}_\sigma$ from (5). Based on the knowledge of ζ and choice of α_σ, the solution of (6a) should satisfy (6b), which is important

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.2021.3055222, IEEE Transactions on Smart Grid

for stability analysis (cf. Appendix B). A numerical algorithm to solve the set of inequalities (6a) is in Appendix A.

To appropriately design the switching signal $\sigma(\cdot)$, the following gains are defined:

$$\varrho_M \triangleq \max_{\sigma\in\Omega} \lambda_{\max}(P_\sigma),\ \ \varrho_m \triangleq \min_{\sigma\in\Omega} \lambda_{\min}(P_\sigma), \tag{7}$$

Following Definition 1, let us consider the switching signal $\sigma(\cdot)$ with an average dwell time ϑ satisfying

$$\vartheta > \vartheta^* = \ln \mu/\kappa, \tag{8}$$

$$\text{where } \mu \triangleq \varrho_M/\varrho_m,\ 0<\kappa<\iota_m/\varrho_M,\ \iota_m \triangleq \min_{\sigma\in\Omega}\{\iota_\sigma\}.$$

Overall Control Structure: Summarizing, the design steps of the proposed control law are enumerated in Algorithm 1.

Algorithm 1 Design steps of the proposed controller

Step 1 (control gains): design suitable matrices $E_\sigma, F_\sigma, L_\sigma$ (cf. Appendix A) such that (6) is satisfied for user-defined scalar α_σ and a given ζ_σ;
Step 2 (switching gains): compute the gains ϱ_M, ϱ_m as (7) and ι_σ as in (6);
Step 3 (ADT switching): the stabilizing switching law has ADT as in (8);
Step 4 (final switched controller): The robust switched WADC strategy is given by (4).

Remark 3 (Controller and Switching law co-design for Implementation): It can be realized from (8) and from Steps 1-3 of Algorithm 1 that design of control and switching laws are interconnected via the gains $E_\sigma, F_\sigma, L_\sigma, P_\sigma, \alpha_\sigma$ and ζ_σ. The standard approach for such co-design is: (i) a desired ϑ is first determined via ADT (2) based on a threat (cyber-attack) perception; (ii) then, the design parameters $E_\sigma, F_\sigma, L_\sigma, P_\sigma$ and α_σ selected to solve (6a); (iii) ι_σ in (6b) is determined based on maximum possible parametric perturbations ζ_σ and (iv) finally, $E_\sigma, F_\sigma, L_\sigma, P_\sigma, \alpha_\sigma$ and ι_σ are tuned to satisfy (8).

The closed-loop stability result is stated as follows:

Theorem 1: Under Assumptions 1-2, the dynamic WADC loop (5) is Uniformly Ultimately Bounded (UUB) by employing the control law (4) and ADT switching law (8), provided the design conditions (6) are satisfied.

Proof. See Appendix B.

IV. Case Study-I

The two-area benchmark system [31], [39] presented in Fig. 1 is adopted to formulate different attack scenarios, and to study the performance of the proposed WADC. The system operates at 400 MW power transfer through tie-line. The various swing modes for this system can be identified as in [40]. PMUs are placed on generator buses and share their measurements over the wide-area communication network. A data integrity attack occurs whenever the PMU measurements are corrupted by hacking into the network. For control design purpose, dynamics (1) are obtained through linearization and model order reduction (cf. [31], [40]).

Contrary to the static loop case, where only one speed difference and one generator are considered for control (namely, the speed difference $\Delta\omega_{(2,4)}$ and the generator G_4), for the proposed WADC we consider all possible pairs in Table I, yielding the set of dynamic loops $\Omega = 1, 2, \ldots, 8$. Note that we consider that any generator that can be equipped with WADC, as this adds an additional redundancy and can be exploited towards improved performance (selecting the most appropriate generator for a given speed difference signal). For simulation, we have selected $\alpha_{\sigma\in\Omega} = \{\alpha_1, \alpha_2, \cdots, \alpha_8\} = \{4, 3.8, 3.5, 3.6, 4.5, 4.6, 5.5, 5.0\} \times 10^2$, $\zeta_\sigma = 0.4\ \forall\sigma$ and $\kappa = 0.9\iota_m/\varrho_M$: these result in $\varrho_M = 105.71, \varrho_m = 7.85$ and ADT $\vartheta^* = 0.98$sec (cf. Algorithm 1). Accordingly, a switching signal $\sigma(t)$ is designed as in Fig. 4, wherein fast switchings (e.g. at $t = 5.25,\ 5.50,\ 6.0,\ 6.8,\ 7.5$ secs) is compensated by slower switchings to satisfy ADT.

In the following, let us call the switching signal in Fig. 4 as original switching signal (OSS). In the reactive scenario, this signal is to be distinguished by the actual switching signal, arising from detecting an attack (detailed later).

Table I
Switching portfolio for two-area system
($\Delta\omega_{(i,j)} = \Delta\omega_i - \Delta\omega_j$)

B_σ	G_1	G_2
C_σ	$\Delta\omega_{(1,3)}$ $(\sigma=1)$ $\Delta\omega_{(1,4)}$ $(\sigma=2)$	$\Delta\omega_{(2,3)}$ $(\sigma=3)$ $\Delta\omega_{(2,4)}$ $(\sigma=4)$
B_σ	G_3	G_4
C_σ	$\Delta\omega_{(1,3)}$ $(\sigma=5)$ $\Delta\omega_{(2,3)}$ $(\sigma=7)$	$\Delta\omega_{(1,4)}$ $(\sigma=6)$ $\Delta\omega_{(2,4)}$ $(\sigma=8)$

A. Reactive Scenarios

We present comparative studies using two reactive scenarios: false data injection and denial-of-services (DOS) attacks.

Reactive Scenario 1) False Data Injection Attack: False data injection to the PMU measured signal is a simple yet dangerous attack. To highlight the impact of the attack for a static loop case, a false data injection attack is designed as a pulse injection to measurement as shown in Fig. 5. The performances of the static [40] (with feedback signal and actuation node as therein) and the proposed WADC are studied in case of oscillation generated by a pulse change in mechanical input power from turbine for G_1 at 5 sec. Before the change, the system is at steady-state. The attack is activated at 8 sec, i.e., 3 sec after the oscillation started.

Results and analysis: From Fig. 6(a) it can be noted that in the interval $t \in [5\ \ 8)$ sec, before the attack started, the static loop WADC was damping the oscillation effectively. However, occurrence of the attack destabilizes the system. On the other hand, the proposed switched WADC strategy switches from $\sigma = 3$ to $\sigma = 2$ at $t = 8$ sec when the attack is detected, thus anticipating the switching scheduled at $t = 8.5$ sec in the OSS (cf. Fig. 4). This results in a modified switching law as depicted in Fig. 6(b). It is evident from Fig. 6(a) that the proposed WADC scheme is able to damp out the oscillations.

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.2021.3055222, IEEE Transactions on Smart Grid

With respect to optimality/robustness trade-off, it is important to mention that, here and in all subsequent simulations, we purposefully selected a lower LSI loop in the steady-state, even before the attack is initiated. This is done to simulate practical scenario where steady-state might arise at lower LSI loop because of some previous attack. As a consequence, the proposed WADC, exhibits suboptimal performance (larger transient), but better robustness against attacks.

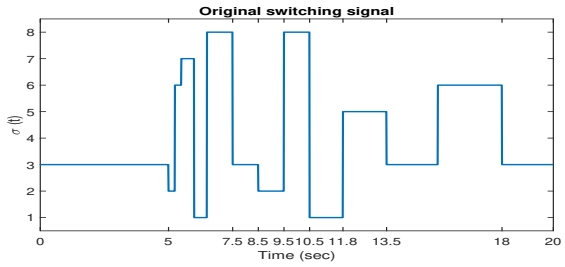


Figure 4. Original switching signal (OSS).

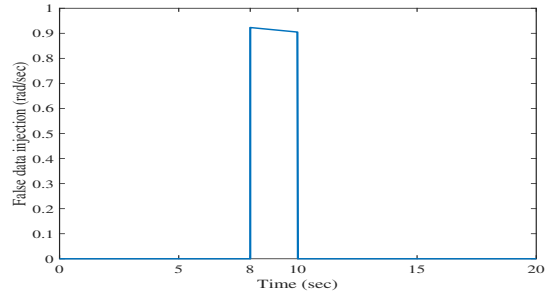
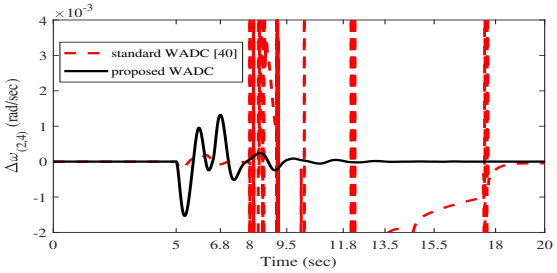
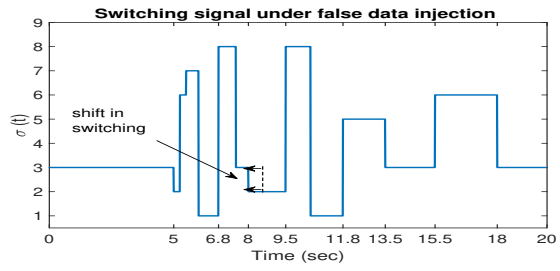


Figure 5. False data injection



(a)



(b)

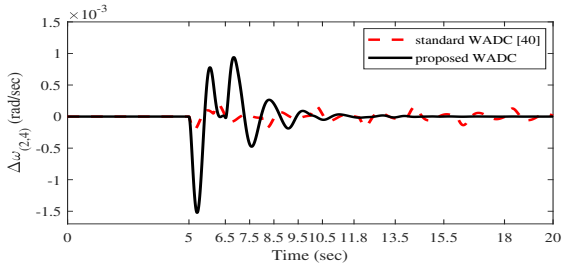
Figure 6. (a) Performance comparison of the controllers and (b) modified switching signal due to attack detection, under false data injection.

Reactive Scenario 2) DoS Attack: In denial-of-service attack, the adversary makes the system to believe that there is a communication overload which results in a temporary signal transmission restriction. To create a DoS attack, the communication for $\Delta\omega_1$ is jammed at 6 sec for 2 sec, i.e., for $6 \leq t \leq 8$ new measurements are blocked. As a result, the measurement $y(t)$ becomes

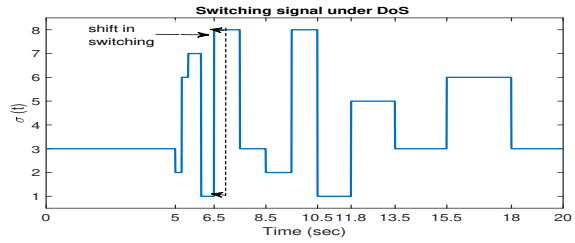
$$y(6 \leq t < 8) = y(6) \text{ and } y(t) = y(t-2) \text{ for } t \geq 8,$$

creating a delay in the loop. As before, a pulse change in G_1 is created at 5 sec.

Results and analysis: Fig. 7 reveals that the static WADC gets affected by the attack, as a sustained oscillation arises. On the other hand, we simulate that the DoS attack is detected after 0.5 sec using the time stamps in the PMU measurements, so that the proposed WADC can switch from $\Delta\omega_{(1,3)}$ ($\sigma = 1$) to $\Delta\omega_{(2,4)}$ ($\sigma = 8$) at $t = 6.5$ sec, anticipating the switching of the OSS. Consequently, the DoS is bypassed and the oscillation damped.



(a)



(b)

Figure 7. (a) Performance comparison of the controllers and (b) modified switching signal due to attack detection, under DoS.

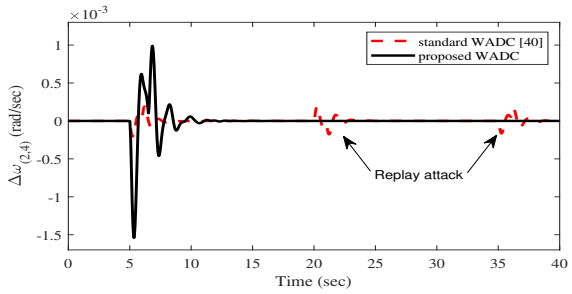
B. Pro-active Scenarios

As compared to a reactive scenario, corrupted data cannot be avoided in case of a stealthy attack and, stability completely relies on pro-actively designing the OSS. The OSS cannot be altered. In the following, we consider two stealthy attack scenarios, namely replay attack and bias injection attack.

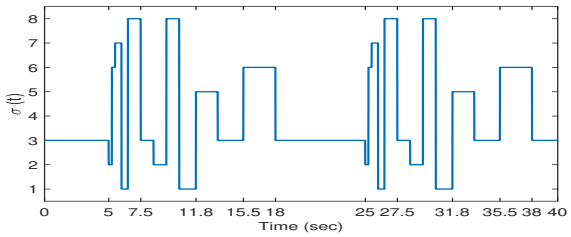
Pro-active Scenario 1) Replay Attack: In replay attacks, an attacker injects false data into the system, where the false data is a mirror image of previously valid measurements. To simulate a replay attack, we copy the measurements when there was a disturbance at $t = 5$ sec in the mechanical input of G_2. Second, we inject such disturbances into the measurement at $t = 20$ sec and $t = 35$ sec when, in reality, there was no disturbance. As before, a pulse in G_1 is created at 5 sec.

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.2021.3055222, IEEE Transactions on Smart Grid

Results and analysis: In Fig. 8, we see that the static loop WADC reacts to the injected data, resulting in transient oscillations even if there is no disturbance. On the other hand, via the dynamic loop strategy of Fig. 8(a), the proposed WADC could avoid such unwanted transients.

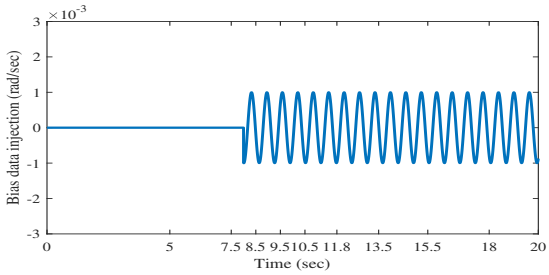


(a)

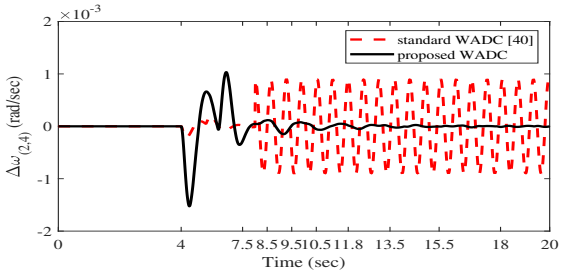


(b)

Figure 8. (a) Performance comparison of the controllers under replay attack and (b) the original switching signal (OSS).



(a)



(b)

Figure 9. (a) Bias injection attack and (b) Performance comparison of the controllers under such attack.

Pro-active Scenario 2) Bias Injection Attack: Bias injection attack may be the result of zero dynamics attack [41]. We considered a persistent bias injection as in Fig. 9(a).

Results and analysis: Figure 9(b) reveals that the proposed dynamic loop based strategy can retain the stability as well as the damping capability, whereas, the damping capability is completely lost for the static loop WADC [40]. Such performance difference can be attributed to the fact that, as opposed to the static loop strategy, the proposed WADC uses "less often" the corrupted signal due to switching in the loop.

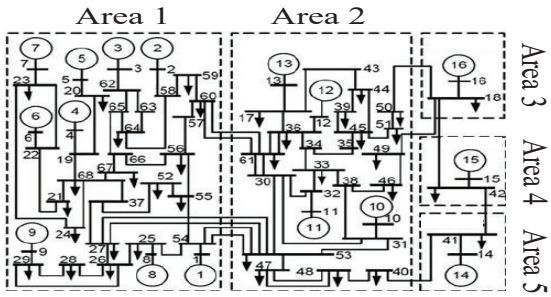


Figure 10. Single line diagram of 16-machine 68-bus system.

V. Case Study-II

For second case study, we consider a 16-machine 68-bus system (Fig. 10) having five areas. The five areas represent: New England (Area 1), New York (Area 2), and three aggregated areas (Area 3, 4 and 5) represented by an aggregated bus and generator. Local PSS are installed from G_1 to G_9 to damp the local oscillatory modes. The detailed system parameter is noted in Power System Toolbox.

Owing to the large number of machines, there can be many possible loops that can be used to control the inter-area oscillations. As G_{14}, G_{15} and G_{16} are aggregated generators they cannot be used for WADC. Therefore, the four synchronous machines with higher participation in the inter-area modes are calculated as $\{G_4,\ G_5,\ G_9,\ G_{10}\}$, which are selected to design wide-area damping controller.

To construct the dynamic loops, the input-output pairs are selected according to Table II, yielding the set of dynamic loops $\Omega = 1, 2, \ldots, 8$. The OSS is designed as in Fig. 11); other control parameters are kept similar to Case Study-I. For comparison, instead of the static WADC in [40], a static robust WADC [35] is used. The robust static WADC in [35] has been selected to further illustrate the trade-off between optimality and robustness. Further, we have compared the proposed WADC with other resilient controllers [42]–[44], designed specifically for some classes of attacks, but applicable to all like the proposed one. The methods in [35], [42]–[44] still use a static loop with $\Delta\omega_{(5,10)}$ as output and the generator G_{10} as input.

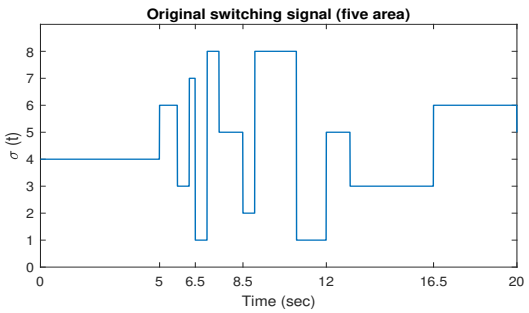


Figure 11. Original switching signal (OSS) for 16-machine 68-bus system.

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.2021.3055222, IEEE Transactions on Smart Grid

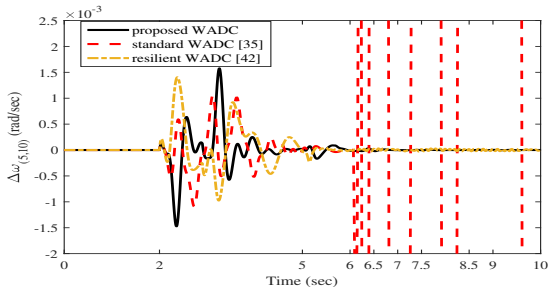
Table II
SWITCHING PORTFOLIO FOR 16-MACHINE 68-BUS SYSTEM
($\Delta\omega_{(i,j)} = \Delta\omega_i - \Delta\omega_j$)

B_σ	G_4	G_5
C_σ	$\Delta\omega_{(4,9)}$ ($\sigma = 1$)	$\Delta\omega_{(5,4)}$ ($\sigma = 5$)
	$\Delta\omega_{(4,5)}$ ($\sigma = 2$)	$\Delta\omega_{(9,5)}$ ($\sigma = 6$)
	$\Delta\omega_{(4,11)}$ ($\sigma = 3$)	$\Delta\omega_{(5,11)}$ ($\sigma = 7$)
	$\Delta\omega_{(10,4)}$ ($\sigma = 4$)	$\Delta\omega_{(10,5)}$ ($\sigma = 8$)
B_σ	G_9	G_{10}
C_σ	$\Delta\omega_{(9,4)}$ ($\sigma = 9$)	$\Delta\omega_{(9,10)}$ ($\sigma = 13$)
	$\Delta\omega_{(4,9)}$ ($\sigma = 10$)	$\Delta\omega_{(4,10)}$ ($\sigma = 14$)
	$\Delta\omega_{(3,9)}$ ($\sigma = 11$)	$\Delta\omega_{(5,10)}$ ($\sigma = 15$)
	$\Delta\omega_{(10,9)}$ ($\sigma = 12$)	$\Delta\omega_{(10,11)}$ ($\sigma = 16$)

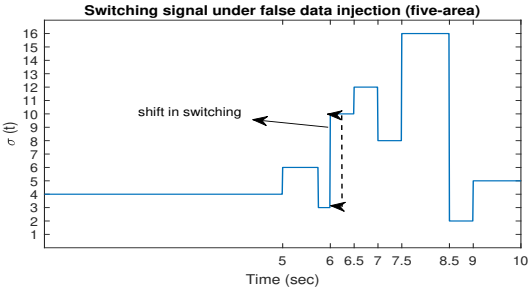
A. Reactive Scenarios

Reactive Scenario 1) False Data Injection Attack: We used similar (in amplitude) pulse false data injection as in Fig. 5 to measurement of $\Delta\omega_{10}$ to simulate the attack. Oscillation is generated by a pulse in mechanical input power from turbine for G_7 at 2 sec. Before the pulse, the system is at steady-state. The attack is activated 4 sec after the oscillation at $t = 6$.

Results and analysis: Figure 12(a) depicts that occurrence of the attack destabilizes the system for the static loop WADC, whereas the proposed WADC is able to damp out the oscillations by switching from $\sigma = 3$ to $\sigma = 7$ at $t = 6$ sec when the attack is detected. Such anticipated switching compared to the switching scheduled at $t = 6.25$ sec in the OSS (cf. Fig. 11), resulted in a modified switching law as in Fig. 12(b). As compared to [42], the proposed WADC provides faster damping but with slightly higher overshoot.



(a)



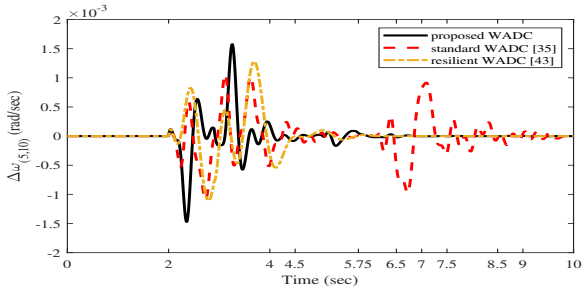
(b)

Figure 12. (a) Performance comparison of the controllers and (b) modified switching signal for 16-machine 68-bus system, under false data injection.

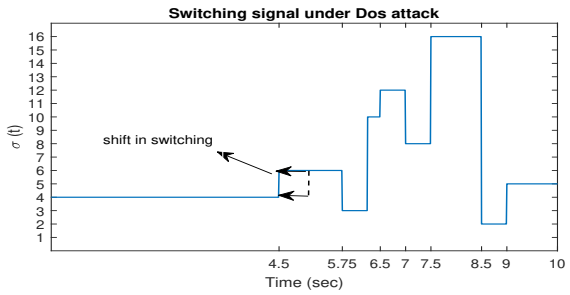
Reactive Scenario 2) DoS Attack: In addition to a pulse in G_7 at $t = 2$ sec, the communication for $\Delta\omega_{10}$ is jammed at 4 sec to create a DoS attack as

$$y(4 \le t < 6) = y(4) \text{ and } y(t) = y(t-2) \text{ for } t \ge 6$$

Results and analysis: Figure 13(a) reveals that the static WADC suffers a sustained oscillation for $t = 4 - 6$ sec, when the data is fixed under the DoS attack. Thereafter, when the delayed measurements is used in feedback, a growing oscillation appears. On the other hand, detecting the DoS attack after 0.5 sec using the time stamps in the PMU measurements, the proposed WADC switches from $\sigma = 4$ to $\sigma = 6$ at $t = 4.5$ sec, before the scheduled switching at $t = 5$ sec in the OSS. This stems a modified switching signal as in Fig. 13(b) and consequently, the oscillation is damped bypassing the DoS. Compared to [43], the proposed WADC has faster response but with slightly higher overshoot.



(a)



(b)

Figure 13. (a) Performance comparison of the controllers and (b) modified switching signal for 16-machine 68-bus system, under DoS.

B. Pro-active Scenarios

Pro-active Scenario 1) Replay Attack: To simulate a replay attack, we copy the measurements when there was a disturbance at $t = 2$ sec in the mechanical input of G_7. Then, we inject such disturbances periodically at 10 sec intervals from $t \ge 2$ sec even if there was no disturbance.

Results and analysis: It can be noted from Fig. 14 that the static loop WADC reacts every time to the injected data causing transient oscillations even if there is no disturbance. Further, both spread and magnitude of oscillations increase with each injection due to residue effect. On the other hand, via the dynamic loop strategy, the proposed WADC could avoid such unwanted transients.

Pro-active Scenario 2) Bias Injection Attack: We used the similar bias as in the previous case study (cf. Fig. 9(a)) to simulate the bias injection attack.

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.2021.3055222, IEEE Transactions on Smart Grid

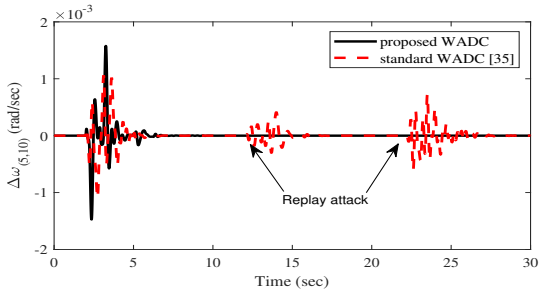


Figure 14. Responses of static and dynamic loop WADC replay attack for 16-machine 68-bus system.

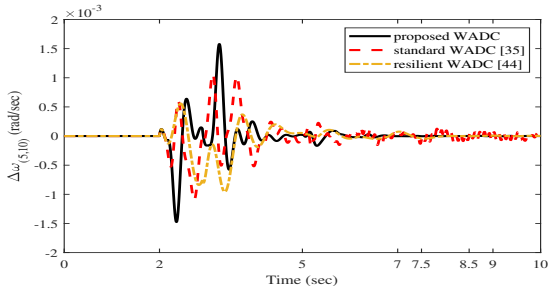


Figure 15. Responses of static and dynamic loop WADC under bias injection attack for 16-machine 68-bus system.

Results and analysis: Figure 15 reveals that the proposed dynamic loop based strategy can retain the stability as well as the damping capability, whereas, the damping capability is completely lost for the static loop WADC. Compared to [44], the proposed WADC has faster response and better settling time, at the cost of higher overshoot.

We have explained that robustness in [35] is intended as capability or "rejecting" some classes of attack, which is done at the cost of decreasing transient performance. As a result, the transient performance of the proposed method is comparable to the one of [35]. This further highlights the trade-off optimality/robustness. Finally, it is worth remarking that the proposed method favourably compares against *all* the state-of-the-art resilient controllers [42]–[44] (faster damping and better settling time, usually at the cost of slightly higher overshoots). The crucial difference is that a *single* flexible and versatile WADC strategy was proposed that can handle all classes of attacks, instead of ad-hoc strategies [35], [42]–[44] that can handle only one class.

VI. Conclusions and Future Work

In this work, a dynamic loop-based robust WADC strategy was proposed under cyber-attack scenarios. The primary feature of the proposed controller resilience is designed without relying on the nature of the attack. For a detectable attack (reactive), the '(feedback signals, actuation node)' pair (or loop) switches to another pair upon detection, while for a stealth attack (pro-active) scenario, such switching occurs based on a user-defined switching law. Using IEEE benchmarks, effectiveness of the proposed scheme was validated against state-of-the-art static loop schemes. The idea of switching dynamically is not limited to attacks, and potentially it can be adopted when fault on one line requires to switch to a different pair (feedback signal, generator) to maintain WADC capabilities. A challenging future work would be to enhance the proposed concept for DAE power network models and include situations such as communication delays and false alarms.

Appendix A
Solution of E_c, L_c, F_c

Let $P_\sigma = \begin{bmatrix} S_\sigma & Q_\sigma \\ Q_\sigma^T & M_\sigma \end{bmatrix}$, $P_\sigma^{-1} = \begin{bmatrix} R_\sigma & U_\sigma \\ U_\sigma^T & N_\sigma \end{bmatrix}$, $X_\sigma = \begin{bmatrix} R_\sigma & I \\ U_\sigma^T & 0 \end{bmatrix}$, and $Y_\sigma = \begin{bmatrix} I & S_\sigma \\ 0 & Q_\sigma^T \end{bmatrix}$. Here, $P_\sigma X_\sigma = Y_\sigma$.

Pre- and post-multiplying (6a) with X_σ yield

$$\begin{aligned} & X_\sigma^T(\overline{A}_\sigma^T P_\sigma + P_\sigma \overline{A}_\sigma)X < -\alpha_\sigma P_\sigma \\ \implies & (Y_\sigma^T \overline{A}_\sigma X_\sigma)^T + Y_\sigma^T \overline{A}_\sigma X_\sigma < -\alpha_\sigma P_\sigma \\ \implies & \begin{bmatrix} L_{11} & L_{12} \\ L_{21} & L_{22} \end{bmatrix} + \begin{bmatrix} L_{11} & L_{12} \\ L_{21} & L_{22} \end{bmatrix}^T < 0 \end{aligned}$$

where $L_{11} = AR_\sigma + B_\sigma L_{c\sigma} U_\sigma^T$, $L_{12} = A$, $L_{21} = S_\sigma^T AR_\sigma + S_\sigma^T B_\sigma L_{c\sigma} U_\sigma^T + Q_\sigma F_{c\sigma} C_\sigma R_\sigma + Q_\sigma E_{c\sigma} U_\sigma^T$ and $L_{22} = S_\sigma^T A + Q_\sigma F_{c\sigma} C_\sigma$

$$\begin{bmatrix} M_{11} & M_{12} \\ M_{12}^T & M_{22} \end{bmatrix} < 0 \tag{9}$$

where $M_{11} = (AR_\sigma + B\hat{L}_{c\sigma}) + (AR_\sigma + B\hat{L}_{c\sigma})^T + \alpha_\sigma S_\sigma$, $M_{12} = A^T + A + \alpha_\sigma Q_\sigma$, $M_{22} = (S_\sigma A + \hat{F}_{c\sigma} C_\sigma)^T + (S_\sigma A + \hat{F}_{c\sigma} C_\sigma) + \alpha_\sigma I$, $\hat{A}_\sigma = S_\sigma^T AR_\sigma + S_\sigma^T B_\sigma L_{c\sigma} U_\sigma^T + Q_\sigma F_{c\sigma} C_\sigma R_\sigma + Q_\sigma E_{c\sigma} U_\sigma^T$, $\hat{F}_{c\sigma} = Q_\sigma F_{c\sigma}$, $\hat{L}_{c\sigma} = L_{c\sigma} U_\sigma^T$. As the decision variables are now linear inequalities, (9) can be solved using linear matrix inequality (LMI) methods, e.g. via the LMI Toolbox of MATLAB. The decision variables can be used to construct the controller matrices

$$\begin{aligned} E_{c\sigma} = Q_\sigma^{-1}(\hat{A}_\sigma - S_\sigma^T AR_\sigma + S_\sigma^T B_\sigma L_{c\sigma} U_\sigma^T \\ + Q_\sigma F_{c\sigma} C_\sigma R_\sigma)(U_\sigma^T)^{-1}, \end{aligned} \tag{10a}$$

$$L_{c\sigma} = \hat{L}_{c\sigma}(U_\sigma^T)^{-1}, \; F_{c\sigma} = Q_\sigma^{-1} F_{c\sigma}. \tag{10b}$$

It took 6.2 sec to solve (offline) LMIs in MATLAB (with Intel i7 processor) for the four the machine scenario in Section IV and 11.6 sec for the sixteen machine scenario in Section V.

Appendix B
Proof of Theorem 1

The stability of the closed-loop system (5) is analysed using the following Lyapunov function:

$$V(t) = \chi^T(t) P_{\sigma(t)} \chi(t), \tag{11}$$

which satisfies (6a). Owing to different choices of P_σ under different σ, $V(t)$ in (11) might be discontinuous at the switching instants and only remains continuous during the time interval between two consecutive switchings. Let an active subsystem be $\sigma(t_{k+1}^-)$ when $t \in [t_k \;\; t_{k+1})$ and $\sigma(t_{k+1})$ when $t \in [t_{k+1} \;\; t_{k+2})$. We have before and after switching

$$V(t_{k+1}^-) = \chi^T(t_{k+1}^-) P_{\sigma(t_{k+1}^-)} \chi(t_{k+1}^-) \tag{12}$$

$$V(t_{k+1}) = \chi^T(t_{k+1}) P_{\sigma(t_{k+1})} \chi(t_{k+1}) \tag{13}$$

respectively. Thanks to the continuity of the state χ in (5) we have $\chi(t_{k+1}^-) = \chi(t_{k+1})$. Further, we have $\chi^T(t) P_{\sigma(t)} \chi(t) \leq$

$\varrho_M \chi^T(t)\chi(t)$ and $\chi^T(t)P_{\sigma(t)}\chi(t) \geq \varrho_m \chi^T(t)\chi(t)$. Then, using these results and (12), (13) one has

$$V(t_{k+1}) - V(t_{k+1}^-) = \chi^T(t_{k+1}^-)(P_{\sigma(t_{k+1})} - P_{\sigma(t_{k+1}^-)})\chi(t_{k+1}^-)$$
$$\leq \left(\frac{\varrho_M - \varrho_m}{\varrho_m}\right) V(t_{k+1}^-) \Rightarrow V(t_{k+1}) \leq \mu V(t_{k+1}^-), \quad (14)$$

with $\mu = \varrho_M/\varrho_m \geq 1$. To study the behaviour of $V(t)$ between two consecutive switching instants, i.e., when $t \in [t_k \;\; t_{k+1})$, let us denote the active subsystem $\sigma(t_{k+1}^-)$ by s.

Using (5) and (6a), the time derivative of V yields (time dependence will be omitted for compactness)

$$\dot{V} = \dot{\chi}^T P_s \chi + \chi^T P_s \dot{\chi} < -\alpha_s \chi^T P_s \chi + 2\chi^T P_s(\Delta \overline{A}_s \chi + \overline{W}_s)$$
$$\leq -[\alpha_s \lambda_{\min}(P_s) - 2||P_s||\zeta_s]\chi^T\chi + 2\overline{w}||P_s||||\chi||$$
$$= -\iota_s \chi^T \chi + 2\overline{w}||P_s||||\chi||. \quad (15)$$

The definition (11) yields $V \leq \varrho_M \chi^T\chi$ and $V \geq \varrho_m \chi^T\chi$. Then, since $\iota_\sigma > 0$ via design (6b), $\dot{V}$ from (15) simplifies to

$$\dot{V} \leq -(\iota_m/\varrho_M)V + (2\overline{w}\varrho_M/\sqrt{\varrho_m})\sqrt{V}$$
$$= -\kappa V - ((\iota_m/\varrho_M) - \kappa)V + (2\overline{w}\varrho_M/\sqrt{\varrho_m})\sqrt{V}, \quad (16)$$

where κ is a scalar defined as $0 < \kappa < \iota_m/\varrho_M$. Therefore, it can be verified from (16) that $\dot{V} < -\kappa V$ when

$$V \geq \max_{s\in\Omega}\left(\frac{2\overline{w}\varrho_M}{\sqrt{\varrho_m}((\iota_m/\varrho_M) - \kappa)}\right)^2 \triangleq \mathcal{B}. \quad (17)$$

In light of this, further analysis is needed to observe the behaviour of $V(t)$ between the two consecutive switching instants, i.e., $t \in [t_k \;\; t_{k+1})$, for two possible scenarios:

(i) when $V(t) \geq \mathcal{B}$, we have $\dot{V}(t) \leq -\kappa V(t)$ implying exponential decrease of $V(t)$;

(ii) when $V(t) < \mathcal{B}$, no exponential decrease can be derived, which are discussed individually below.

Scenario (i): There exists a time, call it T_1, when $V(t)$ enters into the bound $\mathcal{B}$ and $N_\sigma(t)$ denotes the number of all switching intervals for $t \in [0 \;\; T_1)$. Accordingly, for $t \in [0 \;\; T_1)$, using (14) and $N_\sigma(0,t)$ from Definition 1 we have

$$V(t) \leq \exp\left(-\kappa(t - t_{N_\sigma(t)-1})\right) V(t_{N_\sigma(t)-1})$$
$$\leq \mu \exp\left(-\kappa(t - t_{N_\sigma(t)-1})\right)$$
$$\cdot \mu \exp\left(-\kappa(t_{N_\sigma(t)-1} - t_{N_\sigma(t)-2})\right) V(t_{N_\sigma(t)-2}^-)$$
$$\vdots$$
$$= b\left(\exp\left(-\kappa + (\ln\mu/\vartheta)\right)t\right) V(0), \quad (18)$$

where $b \triangleq \exp(N_0 \ln\mu)$. Substituting the ADT condition $\vartheta > \ln\mu/\kappa$ in (18) yields $V(t) < bV(0)$ for $t \in [0 \;\; T_1)$. Moreover, as $V(T_1) < \mathcal{B}$, one has $V(t_{N_\sigma(t)+1}) < \mu\mathcal{B}$ in view of (14). Then, following the recursive argument as in Theorem 1 of [45], one concludes that $V(t) < b\mu\mathcal{B}$ for $t \in [T_1 \;\; \infty)$, i.e., once $V(t)$ enters the interval $[0, \mathcal{B}]$, it cannot exceed the bound $b\mu\mathcal{B}$ any time later with the ADT switching law (8).

Scenario (ii): It can be verified that the same argument below (18) also applies to this scenario.

The stability arguments of Scenarios (i) and (ii) imply that the closed-loop system remains UUB globally (cf. [46] for UUB definition), yielding

$$V(t) \leq \max\{bV(0), b\mu\mathcal{B}\}, \quad \forall t \geq 0. \quad (19)$$

REFERENCES

[1] D. Gautam, V. Vittal, and T. Harbour, "Impact of increased penetration of dfig-based wind turbine generators on transient and small signal stability of power systems," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1426–1434, 2009.

[2] N. Mithulananthan, R. Shah, and K. Y. Lee, "Small-disturbance angle stability control with high penetration of renewable generations," *IEEE Transactions on Power Systems*, vol. 29, no. 3, pp. 1463–1472, 2013.

[3] M. Klein, G. Rogers, and P. Kundur, "A fundamental study of inter-area oscillations in power systems," *IEEE Transactions on Power Systems*, vol. 6, no. 3, pp. 914–921, Aug 1991.

[4] M. E. Aboul-Ela, A. A. Sallam, J. D. Mccalley, and A. A. Fouad, "Damping controller design for power system oscillations using global signals," *IEEE Transaction on Power Systems*, vol. 11, no. 2, pp. 767–773, May 1996.

[5] A. Phadke and R. de Moraes, "The wide world of wide-area measurement," *IEEE Power and Energy Magazine*, vol. 6, no. 5, pp. 52–65, September 2008.

[6] A. Chakrabortty and P. P. Khargonekar, "Introduction to wide-area control of power systems," in *2013 American Control Conference*. IEEE, 2013, pp. 6758–6770.

[7] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1389–1407, 2017.

[8] L. D. Marinovici and H. Chen, "Framework for analysis and quantification of wide-area control resilience for power systems," *IEEE Transactions on Power Systems*, 2019.

[9] Y. Cao, X. Shi, Y. Li, Y. Tan, M. Shahidehpour, and S. Shi, "A simplified co-simulation model for investigating impacts of cyber-contingency on power system operations," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4893–4905, 2018.

[10] Y. Li, Y. Zhou, F. Liu, Y. Cao, and C. Rehtanz, "Design and implementation of delay-dependent wide-area damping control for stability enhancement of power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1831–1842, 2017.

[11] S. Zhang and V. Vittal, "Wide-area control resiliency using redundant communication paths," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2189–2199, 2014.

[12] ——, "Design of wide-area power system damping controllers resilient to communication failures," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4292–4300, 2013.

[13] M. Sarkar, B. Subudhi, and S. Ghosh, "Unified smith predictor based H∞ wide-area damping controller to improve the control resiliency to communication failure," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 2, pp. 584–596, 2020.

[14] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," SANS Ind. Control Syst., Washington, DC, USA, Tech. Rep. MSU-CSE-06-2, March 2016. [Online]. Available: https://www.eisac.com/api/documents/4199/publicdownload

[15] D. Jin, Z. Li, C. Hannon, C. Chen, J. Wang, M. Shahidehpour, and C. W. Lee, "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2494–2504, 2017.

[16] J. Chen, C. Touati, and Q. Zhu, "Optimal secure two-layer IoT network design," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 1, pp. 398–409, 2020.

[17] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.

[18] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636–1646, 2016.

[19] K. Mahapatra, M. Ashour, N. R. Chaudhuri, and C. M. Lagoa, "Malicious corruption resilience in PMU data and wide-area damping control," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 958–968, 2020.

[20] X. Huang, D. Zhai, and J. Dong, "Adaptive integral sliding-mode control strategy of data-driven cyber-physical systems against a class of actuator attacks," *IET Control Theory & Applications*, vol. 12, no. 10, pp. 1440–1447, 2018.

[21] A. Farraj, E. Hammad, and D. Kundur, "A cyber-physical control framework for transient stability in smart grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1205–1215, 2016.

[22] M. Ayar, S. Obuz, R. D. Trevizan, A. S. Bretas, and H. A. Latchman, "A distributed control approach for enhancing smart grid transient stability and resilience," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 3035–3044, 2017.

[23] Y. Shen, W. Yao, J. Wen, H. He, and L. Jiang, "Resilient wide-area damping control using GrHDP to tolerate communication failures," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2547–2557, 2018.

[24] M. Li and Y. Chen, "Wide-area robust sliding mode controller for power systems with false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 922–930, 2020.

[25] M. E. Bento, "Fixed low-order wide-area damping controller considering time delays and power system operation uncertainties," *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 3918–3926, 2020.

[26] ——, "A hybrid procedure to design a wide-area damping controller robust to permanent failure of the communication channels and power system operation uncertainties," *International Journal of Electrical Power & Energy Systems*, vol. 110, pp. 118–135, 2019.

[27] M. E. Bento, D. Dotta, R. Kuiava, and R. A. Ramos, "A procedure to design fault-tolerant wide-area damping controllers," *IEEE Access*, vol. 6, pp. 23 383–23 405, 2018.

[28] S. Khosravani, I. N. Moghaddam, A. Afshar, and M. Karrari, "Wide-area measurement-based fault tolerant control of power system during sensor failure," *Electric Power Systems Research*, vol. 137, pp. 66–75, 2016.

[29] X. Zhou, Z. Gu, and F. Yang, "Resilient event-triggered output feedback control for load frequency control systems subject to cyber attacks," *IEEE Access*, vol. 7, pp. 58 951–58 958, 2019.

[30] X. Zhou and Z. Gu, "Event-triggered H∞ filter design of ts fuzzy systems subject to hybrid attacks and sensor saturation," *IEEE Access*, vol. 8, pp. 126 530–126 539, 2020.

[31] P. Kundur, *Power System Stability and Control*. McGraw Hill Education (India) Private Limited, 2006.

[32] P. R. Sahoo, A. Patel, S. Ghosh, and A. K. Naskar, "Selection of overlapping interaction through approximate decentralized fixed mode measure," *arXiv preprint arXiv:1904.05273*, 2019.

[33] M. Farsangi, Y. Song, and K. Y. Lee, "Choice of FACTS device control inputs for damping interarea oscillations," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 1135–1143, 2004.

[34] A. Hamdan and A. Elabdalla, "Geometric measures of modal controllability and observability of power system models," *Electric Power Systems Research*, vol. 15, no. 2, pp. 147 – 155, 1988.

[35] S. Roy, A. Patel, and I. N. Kar, "Analysis and design of a wide-area damping controller for inter-area oscillation with artificially induced time delay," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3654–3663, 2018.

[36] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[37] J. Milošević, A. Teixeira, K. H. Johansson, and H. Sandberg, "Actuator security indices based on perfect undetectability: Computation, robustness, and sensor placement," *IEEE Transactions on Automatic Control*, 2020.

[38] D. Liberzon, *Switching in systems and control*. Springer Science & Business Media, 2003.

[39] Power System Dynamic Performance Committee, "Benchmark systems for small-signal stability analysis and control," IEEE, Tech. Rep., Aug 2015. [Online]. Available: http://resourcecenter.ieee-pes.org/pes/product/technical-reports/PESTR18

[40] A. Patel, S. Ghosh, and K. A. Folly, "Inter-area oscillation damping with non-synchronised wide-area power system stabiliser," *IET Generation, Transmission & Distribution*, vol. 12, no. 12, pp. 3070–3078, 2018.

[41] G. Park, C. Lee, H. Shim, Y. Eun, and K. H. Johansson, "Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zero-dynamics attack," *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 4907–4919, 2019.

[42] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On detection of false data in cooperative dc microgrids—a discordant element approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, 2019.

[43] R. Ma, P. Shi, and L. Wu, "Dissipativity-based sliding-mode control of cyber-physical systems under denial-of-service attacks," *IEEE Transactions on Cybernetics*, 2020.

[44] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "An event-driven resilient control strategy for dc microgrids," *IEEE Transactions on Power Electronics*, 2020.

[45] S. Roy and S. Baldi, "On reduced-complexity robust adaptive control of switched euler–lagrange systems," *Nonlinear Analysis: Hybrid Systems*, vol. 34, pp. 226–237, 2019.

[46] H. K. Khalil, *Nonlinear systems, 3rd ed.* New Jewsey, Prentice Hall, 2002.

Abhilash Patel (S'13-M'16) received his B.Tech. in Electrical Engineering from Biju Patnaik University of Technology, Rourkela, India and M.Tech. in Control and Automation from National Institute of Technology, Rourkela, India, in 2012 and 2015 respectively. At present, he is a PhD scholar at Indian Institute of Technology Delhi, India in Control and Automation group. His research interests include Wide-Area Control of Power System, Robust Control Theory and Biomolecular Circuit Design.

Spandan Roy received the B.Tech. in Electronics and Communication engineering from Techno India (Salt Lake), West Bengal University of Technology, Kolkata, India, in 2011, the M.Tech. in Mechatronics from Academy of Scientific and Innovative Research, New Delhi, India, in 2013, and the Ph.D. in control and automation from Indian Institute of Technology Delhi, India, in 2018. He is currently Assistant Professor with Robotics Research Center, International Institute of Information Technology Hyderabad, India. Previously, he was Postdoc Researcher with Delft Center for System and Control, TU Delft, The Netherlands. His research interests include artificial delay based control, adaptive-robust control, switched systems and its applications in Euler–Lagrange systems.

Simone Baldi (M'14, SM'19) received the B.Sc. in electrical engineering, and the M.Sc. and Ph.D. in automatic control engineering from University of Florence, Italy, in 2005, 2007, and 2011. He is professor at School of Mathematics and School of Cyber Science and Engineering, Southeast University, with guest position at Delft Center for Systems and Control, TU Delft, where he was assistant professor. He was awarded outstanding reviewer for *Applied Energy* (2016) and *Automatica* (2017). He is subject editor of *Int. Journal of Adaptive Control and Signal Processing*. His research interests are adaptive and learning systems with applications in unmanned vehicle systems ans smart energy systems.