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

Citation (APA)

Important note
To cite this publication, please use the final published version (if applicable). Please check the document version above.
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 Ukraine’s power system outage due to a cyber-attack which affected more than 20000 customers [14].

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

![Figure 1. Network representation of wide-area damping controller: signals used for control can be compromised by malicious attacks.](image-url)
corresponding to the inter-area mode \( \Delta \omega_{(2,4)} \). For the benchmark two-area system (Fig. 1), the LSI results in selecting \( \Delta \omega_{(2,4)} \) (speed deviation between \( G_3 \) 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 \((\Delta \omega_{(2,4)}, G_3), (\Delta \omega_{(1,4)}, G_3), (\Delta \omega_{(2,3)}, G_1)\) 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:

- 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

\[
\begin{align*}
\dot{x}(t) &= Ax(t) + B_i u_i(t) \\
y_{ij}(t) &= C_{ij} x(t)
\end{align*}
\]

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 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
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, $\sigma(t) : [0, \infty) \rightarrow \Omega$ 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 $(B_\sigma, C_\sigma)$ 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].

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{switching_signal.png}
\caption{A representative switching signal $\sigma$}
\end{figure}

**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 $\bar{\tau}$ if

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

(2)

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

**Remark 1** (Significance of ADT): The notion of ADT in [2] signifies that a short dwell-time $(t_{k+1} - t_k) < \bar{\tau}$ must be compensated by a larger dwell-time, i.e., $(t_{k+1} - t_{k-1}) > \bar{\tau}$ 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., $(t_{k+1} - t_k) < \bar{\tau}$) then it can be compensated later by a larger dwell time; (ii) in a proactive 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

$$\dot{x}(t) = A_{\sigma} x(t) + B_{\sigma}(\cdot) u_{\sigma}(\cdot)(t) + W(t)$$

(3a)

$$y_{\sigma}(t) = C_{\sigma}(\cdot)x(t)$$

(3b)

where $A_{\sigma}(\cdot) = A + \Delta A(t)$ and $B_{\sigma}(\cdot)(t) = B_{\sigma}(t) + \Delta B_{\sigma}(t)$, respectively. The terms $A, B_{\sigma}(t)$ denote known nominal values, while $\Delta A(t), \Delta B_{\sigma}(t)$ 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 by $||W(t)|| \leq \bar{w}$ 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 impulsive 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

$$\dot{x}_c = E_\sigma x_c + F_\sigma y,$$

$$u_\sigma = L_\sigma x_c,$$

(4)

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

$$\dot{x} = (A + \Delta A)x + (B_{\sigma} + \Delta B_{\sigma})L_{\sigma} x_c + W,$$

$$\dot{x}_c = E_\sigma x_c + F_\sigma y,$$

(5)

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

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

(5)

where

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

\[
\varrho_M \triangleq \max_{\sigma \in \Omega} \lambda_{\max}(P_\sigma), \quad \varrho_m \triangleq \min_{\sigma \in \Omega} \lambda_{\min}(P_\sigma),
\]

(7)

Following Definition 1, let us consider the switching signal \( \sigma(\cdot) \) with an average dwell time \( \bar{\varepsilon} \) satisfying

\[
\varrho > \varrho^* = \ln \mu/\kappa,
\]

(8)

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 \( \alpha_\sigma \) and a given \( \zeta_\sigma \);

**Step 2 (switching gains):** compute the gains \( \varrho_M, \varrho_m \) as (7) and \( \iota_\sigma \) as in (6);

**Step 3 (ADT switching):** the stabilizing switching law has ADT as in (5);

**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 \( \zeta_\sigma \). The standard approach for such co-design is: (i) a desired \( \bar{\varepsilon} \) is first determined via ADT (2) based on a threat (cyber-attack) perception; (ii) then, the design parameters \( E_\sigma, F_\sigma, L_\sigma, P_\sigma, \alpha_\sigma \) are selected to solve (6a); (iii) \( \iota_\sigma \) in (6a) is determined based on maximum possible parametric perturbations \( \zeta_\sigma \) and (iv) finally, \( E_\sigma, F_\sigma, L_\sigma, P_\sigma, \alpha_\sigma \) and \( \iota_\sigma \) are tuned to satisfy (8).

The closed-loop stability result is stated as follows:

**Theorem 1:** Under Assumptions 1-2, the dynamic WADC loop (4) 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 1 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 \( \alpha_\sigma \in \Omega = \{ \alpha_1, \alpha_2, \ldots, \alpha_8 \} = \{ 4, 3.8, 3.5, 3.6, 4.5, 4.6, 5.5, 5.0 \} \times 10^2 \), \( \zeta_\sigma = 0.4 \) \( \forall \sigma \) and \( \kappa = 0.95 \varrho_M/\varrho_m \); these result in \( \varrho_M = 105.71, \varrho_m = 7.85 \) and ADT \( \varrho^* = 0.98 \) sec (cf. Algorithm 1). Accordingly, a switching signal \( \sigma(t) \) is designed as in Fig. 2 wherein fast switchings (e.g. at \( t = 5.25, 5.50, 6.0, 6.8, 7.5 \) sec) is compensated by slower switchings to satisfy ADT.

In the following, we call the switching signal in Fig. 2 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>
<thead>
<tr>
<th>( B_\sigma )</th>
<th>( G_1 )</th>
<th>( G_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( C_\sigma )</td>
<td>[ \Delta \omega_{(1,3)} (\sigma = 1) ]</td>
<td>[ \Delta \omega_{(2,3)} (\sigma = 3) ]</td>
</tr>
<tr>
<td>( \Delta \omega_{(1,4)} (\sigma = 2) )</td>
<td>[ \Delta \omega_{(2,4)} (\sigma = 4) ]</td>
<td></td>
</tr>
<tr>
<td>( B_\sigma )</td>
<td>( G_3 )</td>
<td>( G_4 )</td>
</tr>
<tr>
<td>( C_\sigma )</td>
<td>[ \Delta \omega_{(1,3)} (\sigma = 5) ]</td>
<td>[ \Delta \omega_{(1,4)} (\sigma = 6) ]</td>
</tr>
<tr>
<td>[ \Delta \omega_{(2,3)} (\sigma = 7) ]</td>
<td>[ \Delta \omega_{(2,4)} (\sigma = 8) ]</td>
<td></td>
</tr>
</tbody>
</table>

**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 depicted in Fig. 6(b). It is evident from Fig. 6(a) that the proposed switched WADC scheme is able to damp out the oscillations.
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 a 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.

**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 $t = 6.5 \text{ sec}$, anticipating the switching of the OSS. Consequently, the DoS is bypassed and the oscillation damped.

![Switching signal under false data injection](image1)

**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 $t = 5 \text{ sec}$ in the mechanical input of $G_2$. Second, we inject such disturbances into the measurement at $t = 20 \text{ sec}$ and $t = 35 \text{ sec}$ when, in reality, there was no disturbance. As before, a pulse in $G_1$ is created at 5 sec.
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.

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.

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.
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 $\Delta \omega \omega$ 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.

![Figure 12(a)](image)

![Figure 12(b)](image)

Table II

<table>
<thead>
<tr>
<th>$B_0$</th>
<th>$G_4$</th>
<th>$G_5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta \omega (4, 9)$ ($\sigma = 1$)</td>
<td>$\Delta \omega (5, 4)$ ($\sigma = 5$)</td>
<td></td>
</tr>
<tr>
<td>$\Delta \omega (4, 5)$ ($\sigma = 2$)</td>
<td>$\Delta \omega (9, 5)$ ($\sigma = 6$)</td>
<td></td>
</tr>
<tr>
<td>$\Delta \omega (4, 11)$ ($\sigma = 3$)</td>
<td>$\Delta \omega (5, 11)$ ($\sigma = 7$)</td>
<td></td>
</tr>
<tr>
<td>$\Delta \omega (10, 4)$ ($\sigma = 4$)</td>
<td>$\Delta \omega (5, 10)$ ($\sigma = 8$)</td>
<td></td>
</tr>
<tr>
<td>$\Delta \omega (9, 4)$ ($\sigma = 9$)</td>
<td>$\Delta \omega (9, 10)$ ($\sigma = 13$)</td>
<td></td>
</tr>
<tr>
<td>$\Delta \omega (4, 9)$ ($\sigma = 10$)</td>
<td>$\Delta \omega (4, 10)$ ($\sigma = 14$)</td>
<td></td>
</tr>
<tr>
<td>$\Delta \omega (4, 9)$ ($\sigma = 11$)</td>
<td>$\Delta \omega (5, 10)$ ($\sigma = 15$)</td>
<td></td>
</tr>
<tr>
<td>$\Delta \omega (10, 9)$ ($\sigma = 12$)</td>
<td>$\Delta \omega (10, 11)$ ($\sigma = 16$)</td>
<td></td>
</tr>
</tbody>
</table>

$G_7$ at $t = 2$ sec, the communication for $\Delta \omega_{10}$ is jammed at 4 sec to create a DoS attack as

$$y(4 \leq t < 6) = y(4)$$

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.

![Figure 13](image)

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 $t \geq 2$ 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.
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 $P_\sigma = \begin{bmatrix} S_\sigma & Q_\sigma \\ Q_\sigma^T & M_\sigma \end{bmatrix}$, $P_\sigma^{-1} = \begin{bmatrix} R_\sigma & U_\sigma \\ U_\sigma^T & N_\sigma \end{bmatrix}$, $X_\sigma = \begin{bmatrix} R_\sigma \\ I \end{bmatrix}$, 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 (4a) with $X_\sigma$ yield

$$X_\sigma^T (\tilde{A}_\sigma^T P_\sigma + P_\sigma Q_\sigma^T X_\sigma) < -\alpha_\sigma P_\sigma$$

$$\Rightarrow (Y_\sigma^T \tilde{A}_\sigma X_\sigma)^T + Y_\sigma^T \tilde{A}_\sigma X_\sigma < -\alpha_\sigma P_\sigma$$

$$\Rightarrow \begin{bmatrix} L_{11} & L_{12} \\ L_{21} & L_{22} \end{bmatrix} + \begin{bmatrix} L_{11} & L_{21} \\ L_{12} & L_{22} \end{bmatrix}^T < 0$$

where $L_{11} = A R_\sigma + B_c L_c, L_{12} = A$, $L_{21} = S_\sigma^T A R_\sigma + S_\sigma^T B_c L_c U_\sigma^T + Q_\sigma F_c C_c R_\sigma + Q_\sigma F_c E_c U_\sigma^T$ and $L_{22} = S_\sigma^T A + Q_\sigma F_c C_c$

$$\begin{bmatrix} M_{11} & M_{12} \\ M_{T1} & M_{T2} \end{bmatrix} < 0$$

(9)

where $M_{11} = (A R_\sigma + B C_l C_c)^T + (A R_\sigma + B C_l C_c)^T + \alpha_\sigma S_\sigma$, $M_{12} = A^T + A + \alpha_\sigma Q_\sigma$, $M_{T1} = S_\sigma^T A R_\sigma + S_\sigma^T B_c L_c U_\sigma^T + Q_\sigma F_c C_c R_\sigma + Q_\sigma F_c E_c U_\sigma^T$, $F_c = Q_\sigma F_c$, $L_{cc} = L_{cc} U_\sigma^T$. 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

$$E_c = Q_\sigma^{-1} (\tilde{A}_\sigma - S_\sigma^T A R_\sigma + S_\sigma^T B_c L_c U_\sigma^T + Q_\sigma F_c C_c R_\sigma + Q_\sigma F_c E_c U_\sigma^T)$$

$$L_{cc} = \tilde{L}_{cc} (U_\sigma^T)^{-1}, \quad F_c = Q_\sigma^{-1} F_c$$

(10a)

(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:

$$V(t) = \chi^T(t) P_\sigma(t) \chi(t),$$

(11)

which satisfies (6a). Owing to different choices of $P_\sigma$ under different $\sigma$, $V(t)$ 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

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

(12)

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

(13)

respectively. Thanks to the continuity of the state $\chi$ in (5) we have $\chi(t_{k+1}) = \chi(t_{k+1})$. Further, we have $\chi^T(t) P_\sigma(t) \chi(t) \leq$
\[
\varrho_M \chi^T(t) \chi(t) + \chi^T(t) P_\sigma(t) \chi(t) \geq \varrho_m \chi^T(t) \chi(t).
\]
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.2021.3055222, IEEE Transactions on Smart Grid

\[
V(t_{k+1}) - V(t_k) = \chi^T(t_k) [P_M(t_k) - P_\sigma(t_{k-1})] \chi(t_k)
\]
- \left( \frac{\varrho_M - \varrho_m}{\varrho_m} \right) V(t_{k-1}) \Rightarrow V(t_{k+1}) \leq \mu V(t_{k+1}),
\]
with \( \mu = \varrho_M / \varrho_m \geq 1 \). To study the behaviour of \( V(t) \) between two consecutive switching instances, i.e., when \( t \in [t_k, t_{k+1}) \), let us denote the active subsystem \( \sigma(t_k) \) by \( s \). Using (3) and (6), the time derivative of \( V \) yields (time dependence will be omitted for compactness)

\[
\dot{V} = \chi^T P \chi + \chi^T P_s \dot{\chi} < \alpha_s \chi^T P \chi + 2 \chi^T P_s (\Delta \dot{\chi} + s) \leq -\alpha_s \chi^T \chi + 2 \chi^T [P_s] \chi |\chi|.
\]

Using (5) and (6a), the time derivative of \( V \) from (15) simplifies to

\[
\dot{V} = -(\varrho_M / \varrho_m) V + (2 \varrho_M \varrho_m / \varrho_m) \sqrt{V} \leq -\kappa V - ([\varrho_M / \varrho_m] - \kappa)V + (2 \varrho_M \varrho_m) \sqrt{V},
\]
where \( \kappa \) is a scalar defined as \( 0 < \kappa < \varrho_m / \varrho_M \). Therefore, it can be verified from (16) that \( V < -\kappa V \) when

\[
V \geq \max_{s \in \mathcal{F}} \left( \frac{2 \varrho_M \varrho_m}{\varrho_m ([\varrho_M / \varrho_m] - \kappa)} \right)^2 \triangleq \mathcal{B}.
\]
In light of this further analysis, it is needed to observe the behaviour of \( V(t) \) between the two consecutive switching intervals, i.e., \( t \in [t_k, t_{k+1}) \), for two possible scenarios:

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

\[
V(t) \leq \exp \left( -\kappa (t - t_{N_s(t)-1}) \right) V(t_{N_s(t)-1}) \leq \mu \exp \left( -\kappa (t - t_{N_s(t)-1}) \right) \cdot \exp \left( -\kappa (t_{N_s(t)-1} - t_{N_s(t)-2}) \right) \cdot \ldots \cdot \exp \left( -\kappa (t_{N_s(t)-2} - t_{N_s(t)-3}) \right) \cdot \ldots \cdot \exp \left( -\kappa (t_0 - t_{N_s(t)-1}) \right) V(t_{N_s(t)-1}) \leq b \exp \left( -\kappa + (\ln \mu / \varrho) \right) t V(0),
\]
where \( b \triangleq \exp \left( N_\sigma(0) \ln \mu \right) \). Substituting the ADT condition \( \varrho > \ln \mu / \kappa \) in (18) yields \( V(t) < bV(0) \) for \( t \in [0, T_1) \). Moreover, as \( V(T_1) < B \), one has \( V(t_{N_s(t)+1}) < b \mathcal{B} \) in view of (14).

Then, following the recursive argument as in Theorem 1 of [45], one concludes that \( V(t) < b \mathcal{B} \) for \( t \in [T_1, \infty) \), i.e., once \( V(t) \) enters the interval \([0, \mathcal{B}]\), it cannot exceed the bound \( b \mathcal{B} \) 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

\[
V(t) \leq \max \{ bV(0), b \mathcal{B} \}, \quad \forall t \geq 0.
\]


