Load Altering Attacks Detection, Reconstruction and Mitigation for Cyber-Security in Smart Grids with Battery Energy Storage Systems

Gianmario Rinaldi[1], Michele Cucuzzella[2], Prathyush P. Menon[1], Antonella Ferrara[2] and Christopher Edwards[3]

Abstract

In this paper, a novel scheme inspired by the Super-Twisting Sliding Mode Algorithm (STA) is proposed to detect, reconstruct and mitigate resonance load altering cyber attacks in smart grids. In the existing literature, it has been shown that these attacks are difficult to be detected by the control centre, as they are often characterised by relatively small power oscillations. Nonetheless, they can degrade the energy balance of the smart grid by making the frequency oscillating outside the tolerable limits. These attacks can further bring disruptive consequences, such as widespread blackouts and the disconnection of an area from the grid. In this study, it is shown that Battery Energy Storage Systems (BESSs) controlled by an observer-based STA can effectively mitigate the impact of these attacks on a smart grid. Specifically, an STA observer is created to detect and reconstruct in real-time load altering cyber attacks in a decentralised fashion. The estimation of the attack is then utilised as a set-point for a decentralised STA-based controller to dynamically regulate the output power of the BESS. The simulation results, which account for three possible scenarios, demonstrate the effectiveness of the proposed scheme.

I. Introduction

It is well known that mismatches between supply and demand in a power system induce frequency deviations that might eventually lead to fatal disruptive consequences, such as the disconnection of an area from the grid or even widespread blackouts [1]. Reducing the frequency deviation is considered a control objective of vital importance for the stability of the overall power system and is achieved by the so-called "Load Frequency Control" (LFC), also known as "Automatic Generation Control" (AGC) [1]. Due to the key importance of power infrastructures, over the years, LFC has attracted and inspired many researchers to develop advanced control and estimation schemes (see for instance [2]–[11] and the references therein).

In order to improve the efficiency and reliability of the power system, the strategies proposed in recent years involve a high level penetration and integration of smart meters and automated intelligent devices to perform real-time monitoring and optimal control tasks. However, the trend towards a smarter and more automated power system, together with the consequent integration of communication capabilities, opens the doors for cyber-attacks, making the overall power infrastructures vulnerable in absence of suitable cyber-security strategies for detecting, reconstructing and mitigating the attacks [12]–[14]. In principle, a cyber-attacker can compromise any sector of a smart grid: the generation, the distribution and the consumption [15].

In this paper the attention is focused on the cyber-attacks targeting the consumption, which are called *load altering attacks* [13], [15]. These attacks aim to alter the load demand at the most crucial nodes of the network in order to degrade its stability and cause damage to the power infrastructure, leading to widespread blackouts. This class of attacks can for example alter the load demand in data centres by compromising their servers via bogus computation tasks. Other examples include the direct or indirect attack on the demand side management programs. It is indeed possible to directly compromise the command signals (e.g. switch on/off) sent to smart residential and industrial appliances that join such programs. On the other hand, it is possible to indirectly manipulate controllable loads by fooling the demand side management programs, which aim to minimize energy costs, via bogus price signals [13], [15]. Specifically, in this work resonance load altering attacks are considered [16], which tamper with the load demand according to a resonance source and such that the variation is kept within an admissible interval to evade standard detection strategies. However, although the demand variation is not large enough to be detected, resonance attacks can induce large frequency deviations leading to blackouts [16]. To promptly rectify power imbalances (also due to cyber attacks) between generation and demand in real-time, the Battery Energy Storage Systems (BESSs) is a promising and maturing devise for such a purpose [17]–[19]. Sliding mode (SM) estimation and control techniques [20], [21] have been successfully proposed in the existing literature with application to energy systems, to both robustly estimate and compensate disturbances, faults and attacks, and to stabilise the systems [2], [3], [8], [9], [22]–[24].

[1] Gianmario Rinaldi and Prathyush P. Menon are with The Centre for Future Clean Mobility, College of Engineering, Mathematics, and Physical Sciences, University of Exeter, Exeter, United Kingdom. G.Rinaldi3(P.M.Prathyush)@exeter.ac.uk.

[2] Michele Cucuzzella and Antonella Ferrara are with Department of Electrical, Computer and Biomedical Engineering, University of Pavia, Pavia, Italy. Michele Cucuzzella is also with the Jan C. Willems Center for Systems and Control, ENTEG, University of Groningen, the Netherlands. michele.cucuzzella(antonella.ferrara)@unipv.it.

[3] Christopher Edwards is with College of Engineering, Mathematics, and Physical Sciences, University of Exeter, Exeter, United Kingdom. C.Edwards@exeter.ac.uk.

This is the final version of the accepted paper included in the Proc. of 2022 European Control Conference (ECC22), Imperial College London, UK, July 2022.

TABLE I

LIST OF SYMBOLS AND VARIABLES ADOPTED IN THE PAPER

Turbine-Governor:		
P_{g_i}	(p.u.)	governor power
P_{t_i}	(p.u.)	turbine power
ACE_i	(p.u.)	area control error
u_{PI_i}	(p.u.)	PI control signal
$T_{g_i} = 0.1$	(s)	governor time constant
$T_{t_i} = 0.3$	(s)	turbine time constant
$R_i = 0.05$	(Hz/p.u.)	primary control coefficient
$K_{P_i} = -1.0$	–	PI proportional gain
$K_{I_i} = -1.0$	–	PI integral gain
$\beta_i = 21$	(p.u./Hz)	area frequency feedback
Generator:		
ϑ_i	(rad)	voltage phase angle
Δf_i	(Hz)	frequency deviation
L_i	(p.u.)	load demand
ΔL_i	(p.u.)	load altering attack
P_{ij}	(p.u.)	power flow exchange
$M_i = 10$	($\mathrm{s}^2 \cdot$ p.u.)	inertia
$D_i = 1.0$	(p.u./Hz)	damping coefficient
$\mathcal{N}_i$	–	neighbourhood set
$\gamma_{ij} = 0.2$	(p.u.)	power line susceptance
BESS:		
P_{b_i}	(p.u.)	output power
u_{b_i}	(p.u.)	control input
$T_{b_i} = 0.2$	(s)	time constant

Inspired by both the benefits of the BESS and the SM principles, a novel scheme to achieve cyber security in smart grids is designed in this paper.

Main Contribution: In this paper, a novel scheme to perform an accurate real-time detection and reconstruction of load altering cyber attacks is proposed, inspired by the Super-Twisting Sliding Mode Algorithm (STA) [20]. The attack mitigation is performed by the BESS. The designed scheme is composed of two subsystems. The first system is an STA-based observer, which detects and reconstructs in real-time load altering attacks. The second system, which is an STA-based controller for the BESS, receives as input the estimate of the attack from the observer and it suitably adjusts the output power of the BESS to perform the mitigation. The designed method distinguishes from the existing ones in the literature. Conventionally, cyber attacks detection and mitigation strategies have been focused on deception attacks [25], [26], where the attacker action aims to tamper with the control input of the LFC or with the Area Control Error (ACE). In contrast, in the present paper, the attention is focused on load altering attacks as in [13], [15], [16], [27], [28]. The STA has been successfully used in [22], where an STA-based controller has been designed to adjust the power of a traditional power system (with its turbine and governor) to compensate for load altering attacks. Conversely, in this paper, the STA is used to control the BESS, as the BESS can guarantee a much faster response to compensate for sudden attacks [17]–[19]. Ergo, to the best of the authors' knowledge, the use of STA-based architectures in smart grids to control BESS mitigating load altering attacks is novel, and it has never been proposed before.

Structure of the Paper: The rest of this paper is organised as follows. Section II introduces the state-space representation of the smart grid dynamics and the load altering cyber attack principles. Section III describes the proposed STA-based methodology to detect, reconstruct and mitigate the considered class of cyber-attacks. Section IV presents to the reader numerical simulations to validate the proposed strategy. Section V describes some concluding remarks and possible future research directions.

Notation and Nomenclature: The notation adopted in this paper is standard. For a signal x, $\hat{x}$ denotes its estimate, whilst $\mathrm{sign}(x)$ is the sign of x. For a vector or matrix x, its transpose is represented as x^T, whilst its Euclidean norm is $||x||_2$. The symbol $0_{x\times y}$ denotes a matrix with x rows and y columns and all zero entries. The symbol $\mathrm{Col}(x_i)$ characterises a column vector with its x_i entries. Table I lists the adopted symbols and variables, and it includes the numerical values of the model parameters, the measurement units, and a brief physical meaning.

II. SYSTEM DESCRIPTION

Figure 1 shows the schematic of the i-th area of a smart grid considered in this paper. It comprises of three subsystems: (i) a traditional power source (with its turbine-governor), (ii) a generator and (iii) a BESS. The turbine-governor is equipped

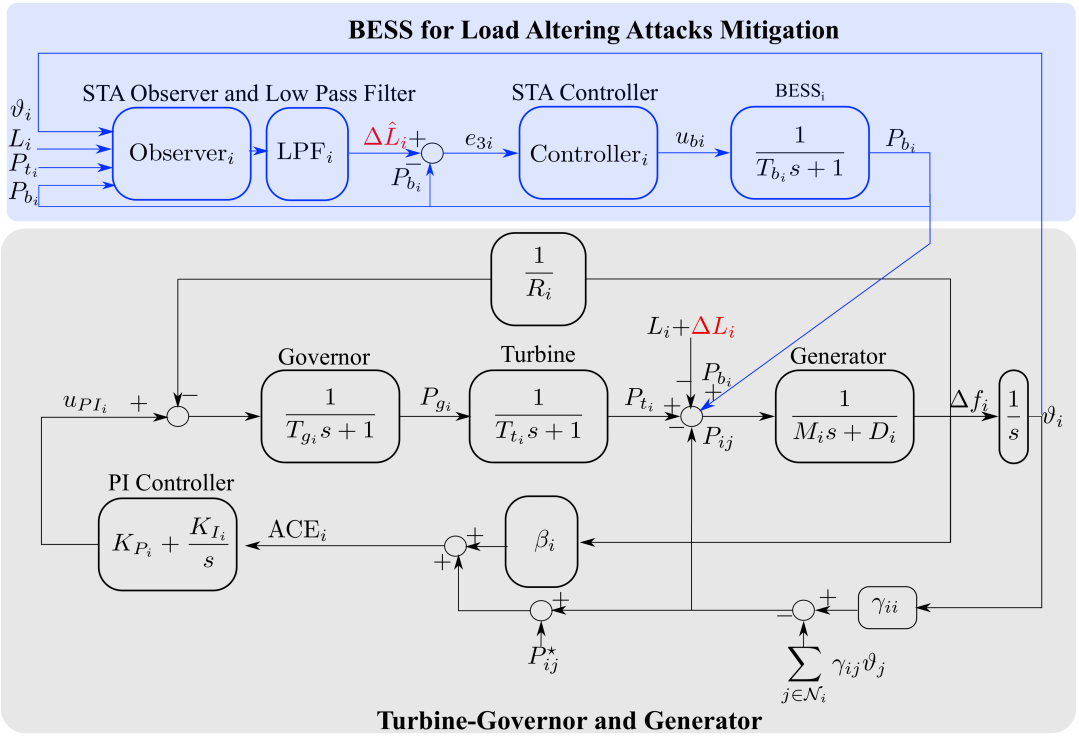

Fig. 1. A schematic of the i-th area of a smart grid, composed of a turbine-governor system, a generator, and a BESS. The action of a load altering cyber attack is depicted in the figure in red.

with a PI controller aiming to regulate the output power of the turbine as a function of the ACE. The proposed BESS includes an STA-based observer and controller. As per Figure 1, the observer generates the reference for the output power of the BESS. The STA-based controller is able to track the generated reference, thus the BESS power is adjusted to compensate for possible load altering cyber attacks.

Given the schematic in Figure 1, the state-space representation of the i-th area of a smart grid can be shown to be [1], [17]

$$\dot{x}_i = A_i x_i + B_i\Big(u_i + p_j\big(x_{j_{|j\in\mathcal{N}_i}}\big)\Big) \tag{1a}$$
$$y_i = C_i x_i, \tag{1b}$$

where $x_i \in \mathbb{R}^5$, $u_i \in \mathbb{R}^3$ and $y_i \in \mathbb{R}^3$ represents the state vector, the input vector and measured output vector of the i-th area of the smart grid. The subscripts G, T and B correspond respectively to the generator, turbine and BESS. The vectors and matrices associated with the system are:

$$x_i := \begin{bmatrix} x_{T_i}^T & x_{G_i}^T & x_{B_i} \end{bmatrix}^T$$
$$x_{T_i} := \begin{bmatrix} P_{g_i} & P_{t_i} \end{bmatrix}^T \quad x_{G_i} := \begin{bmatrix} \vartheta_i & \Delta f_i \end{bmatrix}^T \quad x_{B_i} := P_{b_i}$$

$$A_i := \begin{bmatrix} A_{T_i} & A_{TG_i} & 0_{2\times 1} \\ A_{GT_i} & A_{G_i} & A_{GB_i} \\ 0_{1\times 2} & 0_{1\times 2} & A_{B_i} \end{bmatrix}$$

$$A_{T_i} := \begin{bmatrix} -a_{1i} & 0 \\ a_{2i} & -a_{2i} \end{bmatrix} \quad A_{TG_i} := \begin{bmatrix} 0 & -a_{3i} \\ 0 & 0 \end{bmatrix}$$

$$A_{GT_i} := \begin{bmatrix} 0 & 0 \\ 0 & a_{4i} \end{bmatrix} \qquad A_{G_i} := \begin{bmatrix} 0 & 1 \\ -a_{5i} & -a_{6i} \end{bmatrix}$$

$$A_{GB_i} := \begin{bmatrix} 0 & a_{4i} \end{bmatrix}^T \qquad A_{B_i} := -a_{7i}$$

$$
\begin{aligned}
u_i &:= \begin{bmatrix} u_{T_i} & u_{G_i} & u_{B_i} \end{bmatrix}^T = \begin{bmatrix} u_{PI_i} & L_i & u_{b_i} \end{bmatrix}^T \\
p_j\big(x_{j_{|j\in\mathcal{N}_i}}\big) &:= \begin{bmatrix} 0 & p_j\big(\vartheta_{j_{|j\in\mathcal{N}_i}}\big) & 0 \end{bmatrix}^T
\end{aligned}
$$

$$
\begin{aligned}
B_i &:= \begin{bmatrix} B_{T_i} & 0_{2\times 1} & 0_{2\times 1} \\ 0_{2\times 1} & B_{G_i} & 0_{2\times 1} \\ 0 & 0 & B_{B_i} \end{bmatrix} \\
B_{T_i} &:= \begin{bmatrix} a_{1i} & 0 \end{bmatrix}^T \\
B_{G_i} &:= \begin{bmatrix} 0 & -a_{4i} \end{bmatrix}^T \\
B_{B_i} &:= a_{7i}
\end{aligned}
$$

$$
\begin{aligned}
C_i &:= \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\
y_i &:= \begin{bmatrix} y_{T_i} & y_{G_i} & y_{B_i} \end{bmatrix}^T = \begin{bmatrix} P_{t_i} & \vartheta_i & P_{b_i}. \end{bmatrix}^T
\end{aligned}
$$

Following the details from Table I, the model parameters are: $a_{1i} = 1/T_{g_i}$, $a_{2i} = 1/T_{t_i}$, $a_{3i} = 1/(R_i T_{g_i})$, $a_{4i} = 1/M_i$, $a_{5i} = \gamma_{ii}/M_i$, $a_{6i} = D_i/M_i$, $a_{7i} = 1/T_{b_i}$.

A. Power Flow

Under the state-space representation (1a), the electrical active power flowing from the i-th area to its neighbouring areas $\mathcal{N}_i$ is governed by the relation

$$
P_{ij} = \gamma_{ii}\vartheta_i - \underbrace{\sum_{j\in\mathcal{N}_i} \gamma_{ij}\vartheta_j}_{p_j\left(\vartheta_{j_{|j\in\mathcal{N}_i}}\right)}. \tag{2a}
$$

where the parameter $\gamma_{ii} := \sum_{j\in\mathcal{N}_i} \gamma_{ij}$. Note that the power flow formulated in (2a) is the so-called linearised DC power flow [29]. Nevertheless, the methodology presented in this paper is also applicable to the nonlinear power flow formulation [1]–[3], [5]. Specifically, if the nonlinear power flow method is adopted, P_{ij} becomes:

$$
P_{ij} = \sum_{j\in\mathcal{N}_i} \gamma_{ij} \sin(\vartheta_i - \vartheta_j). \tag{2b}
$$

B. Control Inputs

For the system characterisation given in (1a), an i-th area of the smart grid can be controlled by ***two*** inputs, namely the PI control scheme for the turbine-governor system (u_{PI_i}), and the control scheme for the BESS (u_{b_i}).

PI Control of Turbine-Governor: The PI control of the Turbine-Governor aims to steer to zero the ACE. The ACE is defined as

$$
\mathrm{ACE}_i := \beta_i \Delta f_i + P_{ij} - P_{ij}^\star \tag{3}
$$

where $P_{ij}^\star$ represents the reference value for the power exchange between the i-th area and its neighbourhood. Classically, a standard PI control scheme is employed to asymptotically steer to zero the ACE [1]:

$$
u_{PI_i} = K_{P_i}\mathrm{ACE}_i + K_{I_i} \int \mathrm{ACE}_i \tag{4}
$$

Control of BESS: The BESS is a fast-acting equipment that can store electrical energy and release it when required, in order to promptly regulate the frequency of the smart grid [17]–[19]. In the present paper, the BESSs are employed as a mitigation device and therefore a specific control input will be designed. The aim in this paper is to regulate the BESS to track a power set-point. The power set-point is chosen such that the effect of the load altering cyber attack is effectively mitigated.

C. Load Altering Cyber Attack

The exogenous signal L_i is the nominal load demand. In this study, L_i is considered known, as it represents the received aggregated costumers' power load requests of the i-th area. This quantity is also typically known in advance (e.g. the day-ahead) and updated every 15 minutes via the so-called tertiary control architecture [1]. A load altering cyber attack tampers

with the exogenous power load demand as:

$$\tilde{L}_i := L_i + \Delta L_i, \tag{5}$$

where ΔL_i is the effect of the attack, which can represent a time-varying surplus or shortfall load demand [13], [15]. This action can have a detrimental effect on the LFC of the i-th area of the smart grid causing disruptions of power supply [12]–[14]. In this paper, we consider a class of load altering cyber attacks, named *resonance* attacks, which can be expressed as in [16], i.e.,

$$\Delta L_i := -\mu_i \text{sign}\big(r_i(t-\tau_{L_i})\big), \tag{6}$$

where μ_i and τ_{L_i} are two parameters manipulable by the attacker, and they represent, respectively, the amplitude of the load variation, measured in (p.u.), and the fixed time delay measured in (s). The signal r_i can be designed by using the state variables x_i available to the attacker [16]. For instance, the rate of change of frequency (RoCoF) is utilised in [16], yielding

$$r_i := \Delta \dot{f}_i. \tag{7}$$

The claim in [16] is that such a load altering cyber attack brings both the frequency deviation and the RoCoF outside the values tolerable by the network. Following [13], [15], [16] and the references therein, an underlying assumption here is that the attacker is able to directly or indirectly compromise the smart meters and appliances of the smart grid over the internet and intermittently switch on/off a portion of loads to implement the attack policy in (6) (see Section I and [13], [15], [16] for further details on the implementation of such attacks).

Remark 1 *Note that, in the present study, a specific class of load altering cyber attack, named resonance attacks, has been considered. Nonetheless, the methodology described in the rest of this manuscript is entirely applicable to any types of load altering cyber attacks tampering with the load demand as in* (5)*.*

The compact state-space representation (1a)-(1b) in the presence of load altering cyber attack (6) becomes

$$\dot{x}_i = A_i x_i + B_i\Big(u_i + p_j\big(x_{j_{|j\in\mathcal{N}_i}}\big) + d_i(x_i,t)\Big) \tag{8a}$$

$$y_i = C_i x_i, \tag{8b}$$

where the load altering cyber attack is represented by the vector

$$d_i(x_i,t) := \begin{bmatrix} 0 & \Delta L_i & 0 \end{bmatrix}^T. \tag{8c}$$

D. Assumptions

To design an observer-based STA controller for the BESS, the following assumptions are imposed in the present work:

Assumption 1 *It is assumed that*

(A1) *The resonance attack amplitude is bounded, i.e.:*

$$|\Delta L_i| \leq \Psi_{\Delta L_i}, \tag{9}$$

where $\Psi_{\Delta L_i}$ is a known positive constant.

(A2) *In each area there is a sufficient penetration of BESSs, to ensure that*

$$\max(P_{b_i}) \geq \Psi_{\Delta L_i}. \tag{10}$$

Furthermore, the BESS capacity is sufficiently large to ensure real-time attack compensation without breaching any physical constraints on the state-of-charge of the BESS.

Remark 2 *Assumption 1-(A1) is satisfied due to the bounded load capacity to be tampered with throughout the load altering cyber attack* (5)*. Note that if Assumption 1-(A2) is relaxed, a partial mitigation strategy can still be implemented in the smart grid.*

III. Detection, Reconstruction and Mitigation of load altering cyber attacks

A. Detection and Reconstruction via STA-Based Observer

From the compact representation of the smart grid (8a)-(8b), the generator dynamics alone is:

$$\begin{aligned}\dot{x}_{G_i} = {} & A_{GT_i}x_{T_i} + A_{G_i}x_{G_i} + A_{GB_i}x_{B_i} \\ & + B_{G_i}\Big(p_j\big(\vartheta_{j_{|j\in\mathcal{N}_i}}\big) + u_{G_i} + \Delta L_i\Big).\end{aligned} \tag{11}$$

The STA-based observer for the generator is:

$$\begin{aligned}\dot{\hat{x}}_{G_i} &= A_{GT_i}\tilde{y}_{T_i} + A_{G_i}\hat{x}_{G_i} + A_{GB_i}y_{B_i} \\ &\quad + B_{G_i}\Big(p_j\big(\vartheta_{j_{|j\in\mathcal{N}_i}}\big) + u_{G_i}\Big) + f(e_{G_i}),\end{aligned} \tag{12}$$

where $\hat{x}_{G_i}$ denotes the estimate of x_{G_i} and the auxiliary output measurement vector is $\tilde{y}_{T_i} := [0 \;\; y_{T_i}]^T$. Note that in (12) it has been exploited the structure of the matrix A_{GT_i}, and the identities $A_{GT_i}x_{T_i} \equiv A_{GT_i}\tilde{y}_{T_i}$ and $x_{B_i} \equiv y_{B_i}$. The nonlinear function $f(e_{G_i})$ is [20], [30]:

$$f(e_{G_i}) := \begin{bmatrix} k_{G_{i1}}|e_{G_{i1}}|^{1/2}\text{sign}(e_{G_{i1}}) \\ \\ k_{G_{i2}}\text{sign}(e_{G_{i1}}) \end{bmatrix}, \tag{13}$$

where $e_{G_i} := \hat{x}_{G_i} - x_{G_i} = [e_{G_{i1}} \;\; e_{G_{i2}}]^T$. The design constants $k_{G_{i1}}$ and $k_{G_{i2}}$ are positive, and the tuning rules for them will be provided in the sequel. By subtracting (12) from (11), the error dynamics take the form of

$$\dot{e}_{G_i} = A_{G_i}e_{G_i} + B_{G_i}\Delta L_i - f(e_{G_i}). \tag{14}$$

Due to the structure of matrices A_{G_i} and B_{G_i} in (8a), the system in (14) has the standard form of the STA [30]. Moreover, the dynamics (14) is finite-time stable and it converges to the origin in finite time if the gains satisfy [20]:

$$k_{G_{i1}} = 1.5\sqrt{\Psi_{\Delta L_i}} \tag{15a}$$

$$k_{G_{i2}} = 1.1\Psi_{\Delta L_i}. \tag{15b}$$

The sliding motion is characterised by the following relations $e_{G_{i1}} = e_{G_{i2}} = \dot{e}_{G_{i2}} = 0$. During sliding, the discontinuous term $-k_{G_{i2}}\text{sign}(e_{G_{i1}})$ in the second equation of the system (14) compensates for the load altering cyber attack ΔL_i. Formally,

$$-k_{G_{i2}}\text{sign}(e_{G_{i1}})|_{\text{eq}} = a_{4_i}\Delta L_i, \tag{16}$$

where $-k_{G_{i2}}\text{sign}(e_{G_{i1}})|_{\text{eq}}$ is the average value of the discontinuous signal to maintain the sliding motion. Therefore, an estimate for ΔL_i can be obtained in real-time by low pass filtering [31] the discontinuous signal $-k_{G_{i2}}\text{sign}(e_{G_{i1}})$. The following criteria are in place to perform the resonance attack detection and reconstruction:

$$\Delta\hat{L}_i = \frac{v_{G_i}}{a_{4i}} \tag{17a}$$

$$\Delta\hat{L}_i \rightarrow \begin{cases} \big|\Delta\hat{L}_i\big| \geq \varepsilon_{\Delta L_i} & \text{under attack} \\ \big|\Delta\hat{L}_i\big| < \varepsilon_{\Delta L_i} & \text{no attack,} \end{cases} \tag{17b}$$

where v_{G_i} is a filtered version of $-k_{G_{i2}}\text{sign}(e_{G_{i1}})$, and $\epsilon_{\Delta L_i}$ is an arbitrarily small positive threshold.

Remark 3 *In the present study, it is assumed that $\Delta\hat{L}_i$ is twice differentiable. This feature can be imposed by adopting a second (or higher) order low pass filter to extract $\Delta\hat{L}_i$ from* (17a)*.*

B. Mitigation via STA BESS Control

In order to mitigate the impact of an attack on the i-th area, the estimate of the cyber attack obtained using the STA-based observer is used as the reference for the BESS power. For the state space representation (8a), the following STA control strategy for the BESS is proposed:

$$x^{\star}_{B_i} = \Delta\hat{L}_i \tag{18a}$$

$$s_{B_i} := x^{\star}_{B_i} - x_{B_i} \tag{18b}$$

$$u_{B_i} := u_{B_{i1}} + u_{B_{i2}} + u_{B_{i3}} \tag{18c}$$

$$u_{B_{i1}} := k_{B_{i1}}|s_{B_i}|^{1/2}\text{sign}(s_{B_i}) \tag{18d}$$

$$u_{B_{i2}} := -s_{B_i} \tag{18e}$$

$$\dot{u}_{B_{i3}} = k_{B_{i2}}\text{sign}(s_{B_i}). \tag{18f}$$

Equation (18a) means that the reference for the BESS power should be the estimate of the load altering cyber attack. Defining the tracking error as in (18b), the STA architecture (18c)-(18f) is employed to nullify s_{B_i} in finite time. The positive design constants of the STA controller are $k_{B_{i1}}$ and $k_{B_{i2}}$. By using the i-th area dynamics (8a)-(8b), and introducing the state vector $\sigma_{B_i} := [s_{B_i} \;\; e_{B_i}]^T$, where $e_{B_i} := \Delta\dot{\hat{L}}_i - A_{B_i}\Delta\hat{L}_i - B_{B_i}u_{B_{i3}}$, yields

$$\dot{\sigma}_{B_i} = E_{B_i}\sigma_{B_i} + G_{B_i}\omega_{B_i} + d_{B_i}(\Delta\hat{L}_i), \tag{19}$$

where

$$\begin{aligned} E_{B_i} &:= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad G_{B_i} := \begin{bmatrix} -B_{B_i} & 0 \\ 0 & -B_{B_i} \end{bmatrix} \\ \omega_{B_i} &:= \begin{bmatrix} u_{B_{i1}} & \dot{u}_{B_{i3}} \end{bmatrix}^T \\ d_{B_i}(\Delta\hat{L}_i) &:= \begin{bmatrix} 0 \\ \Delta\ddot{\hat{L}}_i - A_{B_i}\Delta\dot{\hat{L}}_i \end{bmatrix}. \end{aligned}$$

Note that the state-space representation in (19) is obtained after standard algebraic manipulations, using also the relation $A_{B_i} \equiv -B_{B_i}$ from (1a). Under Assumption 1, given the STA-based control scheme (18c)-(18f) and according to Remark 3, it yields

$$\left|\left|d_{B_i}(\Delta\hat{L}_i)\right|\right|_2 \leq \Psi_{B_i}, \tag{20}$$

where Ψ_{B_i} is a known positive constant. The system in equation (19) is again in the standard form of the STA [30]. Provided that $k_{B_{i1}}$ and $k_{B_{i2}}$ are tuned analogously to (15a)-(15b), the dynamics (19) are finite time stable, and the sliding motion $s_{B_i} = e_{B_i} = 0$ is enforced in finite time, which means that the equality $x^{\star}_{B_i} = x_{B_i} = \Delta\hat{L}_i$ is enforced in finite time. To show the effect of the mitigation strategy on the generator dynamics alone, it is possible to rewrite (11) during sliding as $x^{\star}_{B_i} = x_{B_i} = \Delta\hat{L}_i$, i.e.,

$$\begin{aligned} \dot{x}_{G_i} &= A_{GT_i}x_{T_i} + A_{G_i}x_{G_i} + B_{G_i}\Big(- \overbrace{x_{B_i}}^{=\Delta\hat{L}_i} + \Delta L_i \\ &\quad + p_j\big(\vartheta_{j_{|j\in\mathcal{N}_i}}\big) + u_{G_i}\Big), \end{aligned} \tag{21}$$

where the relation $A_{GB_i} = -B_{G_i}$ from (1a) has been utilised. It is clear from (21) that the effect of the load altering cyber attack is mitigated.

Remark 4 *In the stability analysis undertaken in this study, it has been individually proven that the finite-time convergence to the origin of the systems in* (14)*, and* (19) *occurs. In order to ensure that each i-th area of the smart grid is stable during the resonance attack mitigation strategy, the following facts are verified:*

- *By direct calculation, the matrix A_i in* (8a) *is Hurwitz, ergo the dynamical system in* (8a)-(8b) *is Bounded-Input Bounded-State stable [32].*
- *The attack mitigation strategy* (18a)-(18f) *is applied only after the finite-time convergence to the origin of the systems* (14) *and* (19)*.*

Remark 5 *Note that the proposed methodology aims to detect and reconstruct load altering cyber attacks in smart grids and it provides an effective* **mitigation** *strategy applicable in a short-term horizon (i.e. in the order of seconds/minutes). Conversely, the* **recovery** *plan from the attack involves a series of measures in the longer time horizon (i.e. in the order of several minutes) [14], which is outside the scope of the present manuscript.*

Mitigation Metric: The metric $\mathcal{M}_{\Delta f}$ defined as

$$\mathcal{M}_{\Delta f} := \frac{1}{T}\int_0^T \frac{\left|\left|\Delta f\right|\right|_2}{\left|\left|\Delta\hat{L}\right|\right|_2} \tag{22}$$

is introduced to evaluate the performances of the proposed scheme, where $\Delta f := \mathrm{Col}(\Delta f_i)$, $\Delta\hat{L} := \mathrm{Col}(\Delta\hat{L}_i)$, and T is the considered time horizon. Note that $\mathcal{M}_{\Delta f}$ is a global quantity as it accounts for all the areas of the smart grid. $\mathcal{M}_{\Delta f}$ represents the mean value of the ratio between the Euclidean norm of the frequency deviation vector, and the Euclidean norm of the resonance attack estimates vector. The smaller $\mathcal{M}_{\Delta f}$, the more effective is the resonance attack mitigation strategy.

IV. Simulation Results

In this section, the proposed mitigation strategy for resonance attack is assessed via numerical simulations. A smart grid composed of two areas is considered, which is depicted in Figure 2. The numerical values of the model parameters are taken from [16] and reported in Table I. The design constant of each of the STA-based observer (12) are set equal to $k_{G_{i1}} = 1.50,\ k_{G_{i2}} = 1.10$, whilst the design constant for the STA-based controllers (18c)-(18f) are $k_{B_{i1}} = 3.35,\ k_{B_{i2}} = 5.50$. A 2-nd order Butterworth Filter [31], with a bandwidth of 10 Hz, is utilised to extract the resonance attack estimation. The 2-areas smart grid is simulated in a Matlab-Simulink R2020b environment, and the Euler method is employed to perform a fixed-step integration (the sampling frequency is equal to 10 kHz).

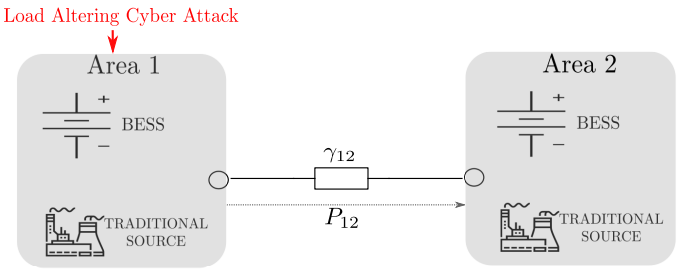

Fig. 2. A schematic of the smart grid considered in the simulations. The system is composed of two interconnected areas. A resonance attack affects Area 1.

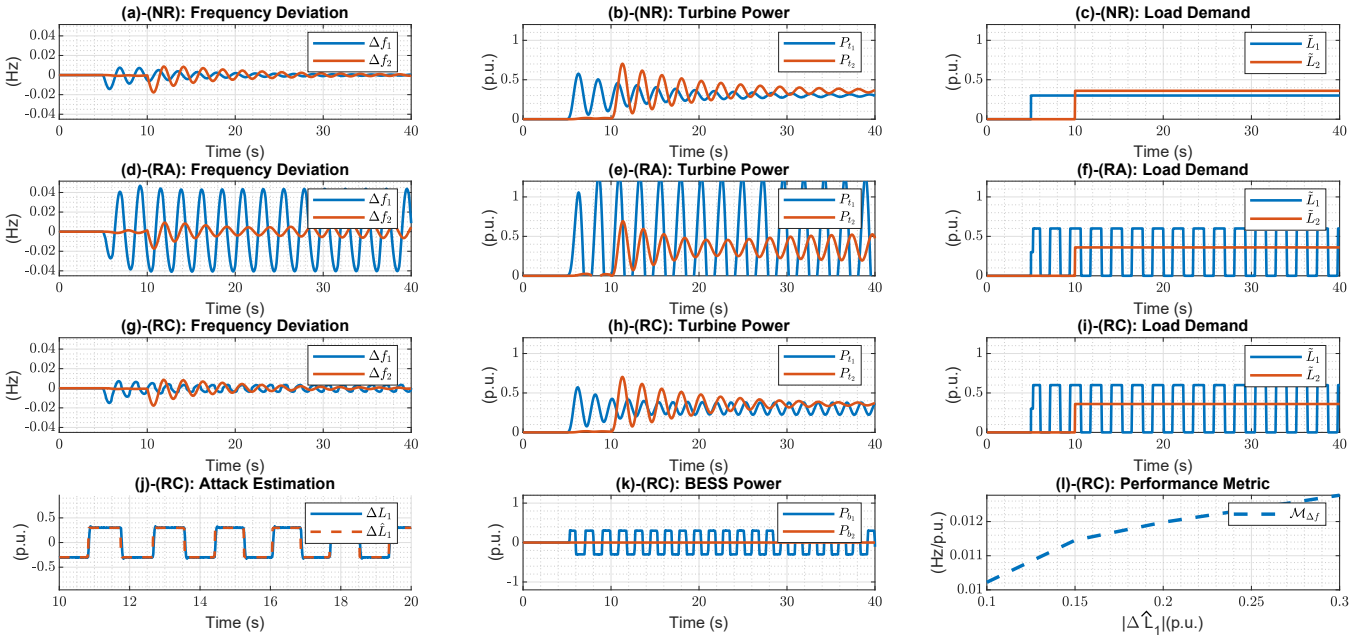

Fig. 3. Time evolution of: **(Scenario NR)**: the frequency deviations, the turbine power and the load demand. **(Scenario RA)**: the frequency deviations, the turbine power and the load demand with the resonance attack. **(Scenario RC)**: the frequency deviations, the turbine powers, the load demands with the resonance attack, the resonance attack reconstructions, the BESS power, and the performance metric for various values of $|\Delta L_1|$.

Three key-scenarios are considered

- **No Resonance Attack Scenario (NR):** There are no resonance attacks affecting the grid. A small load step variation of 0.3 (p.u.) takes place in Area 1 at the time instant $t = 5$ seconds, whilst a similar load step variation of 0.35 (p.u.) takes place in Area 2 at $t = 10$ seconds.
- **Resonance Attack Scenario (RA):** The load step variations characterising Scenario NR still take place. Additionally, a resonance attack is launched in Area 1 at the time instant $t = 5$ and it is governed by

$$\Delta L_1 = -0.3\text{sign}(r_1(t - 0.25)) \tag{23}$$

- **Resonance Attack Compensation Scenario (RC):** The same features of Scenario (RA) are considered, and in addition the proposed detection, reconstruction and mitigation strategy is implemented.

A. *Scenario (NR)*

During this attack-free scenario, unsurprisingly the existing PI frequency controllers of each area are able to bring back to zero the frequency deviation, as shown in Figure 3-(a-b), following the two load step variations depicted in Figure 3-(c).

B. *Scenario (RA)*

If a resonance attack in the form of (23) is launched in Area 1 (see Figure 3-(f)), the frequencies deviates in both the areas. In Area 1, which is the most affected, the peak of Δf_1 exceeds the value of 0.04 Hz, as shown in Figure 3-(d) . Furthermore, the attack sensibly deteriorates the performances of the exiting PI controllers, as noticeable from Figure 3-(e).

TABLE II

PERFORMANCE METRIC FOR SCENARIO (RA) AND (RC). $|\Delta L_1| = 0.3$ (P.U.)

	$\mathcal{M}_{\Delta f}$	
(RA)	0.0810	
(RC)	0.0128	**84%** lower than (RA)

C. Scenario (RC)

The benefits of the proposed BESS-based attack mitigation strategy are evaluated in Scenario (RC). In particular, the frequency deviations are sensibly smaller, as shown in Figure 3-(g). The accurate estimation of the resonance attack is displayed in Figure 3-(j), whilst the time evolution of the output power of the BESS is shown in Figure 3-(k).

D. Performance Metric Results

Table II compares the value of $\mathcal{M}_{\Delta f}$ between Scenario (RA) and (RC). If the mitigation is adopted (Scenario (RC)), the metric is **84%** smaller than Scenario (RA). Furthermore, for Scenario (RC), different values in the interval $[0.1,\ 0.3]$ (p.u) of $|\Delta L_1|$ have been considered. For each of these values, the performance metric $\mathcal{M}_{\Delta f}$ is evaluated and shown in Figure 3-(l).

V. CONCLUSIONS

In this paper, a novel STA-inspired estimation and control scheme has been proposed to detect, reconstruct and mitigate load altering cyber attacks in modern smart grids. The STA has been applied to detect/reconstruct the attack and control the BESS to mitigate its effect by compensating for sudden power fluctuations. The numerical simulations have been focused on three key-scenarios and they have validated the effectiveness of this study. Further research directions, which are being prepared by the authors, can follow starting from the present manuscript. For example, it is worth mentioning the development of SM-based frameworks for control and cyber security, including also other types of cyber attacks.

REFERENCES

[1] M. Eremia and M. Shahidehpour, *Handbook of electrical power system dynamics: modeling, stability, and control*. John Wiley & Sons, 2013, vol. 92.

[2] S. Trip, M. Cucuzzella, C. De Persis, A. van der Schaft, and A. Ferrara, "Passivity-Based Design of Sliding Modes for Optimal Load Frequency Control," *IEEE Transactions on Control Systems Technology*, vol. 27, no. 5, pp. 1893–1906, 2019.

[3] S. Trip, M. Cucuzzella, C. D. Persis, A. Ferrara, and J. M. A. Scherpen, "Robust load frequency control of nonlinear power networks," *International Journal of Control*, vol. 93, no. 2, pp. 346–359, 2020.

[4] S. Trip, M. Bürger, and C. De Persis, "An internal model approach to (optimal) frequency regulation in power grids with time-varying voltages," *Automatica*, vol. 64, pp. 240–253, 2016.

[5] A. Silani, M. Cucuzzella, J. M. A. Scherpen, and M. J. Yazdanpanah, "Output Regulation for Load Frequency Control," *IEEE Transactions on Control Systems Technology*, 2021 (Early Access).

[6] G. Rinaldi, P. P. Menon, C. Edwards, A. Ferrara, and Y. Shtessel, "Adaptive dual-layer super-twisting sliding mode observers to reconstruct and mitigate disturbances and communication attacks in power networks," *Automatica*, vol. 129, 2021.

[7] G. Rinaldi, P. P. Menon, C. Edwards, and A. Ferrara, "Sliding mode observer-based finite time control scheme for frequency regulation and economic dispatch in power grids," *IEEE Transactions on Control Systems Technology*, pp. 1–8, 2021.

[8] ——, "Higher order sliding mode observers in power grids with traditional and renewable sources," *IEEE Control Systems Letters*, vol. 4, no. 1, pp. 223–228, 2019.

[9] P. P. Menon and C. Edwards, "A sliding mode fault detection scheme for corrupted measurement data exchange in a network of dynamical systems," in *Proc. of 52nd IEEE Conference on Decision and Control (CDC)*, Florence, Italy, December 2013, pp. 2852–2857.

[10] F. Dörfler and S. Grammatico, "Gather-and-broadcast frequency control in power systems," *Automatica*, vol. 79, pp. 296–305, 2017.

[11] J. G. Rueda-Escobedo, J. A. Moreno, and J. Schiffer, "Finite-time estimation of time-varying frequency signals in low-inertia power systems," in *Proc of 18th IEEE European Control Conference (ECC)*, Naples, Italy, May 2019, pp. 2108–2114.

[12] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.

[13] S. Mehrdad, S. Mousavian, G. Madraki, and Y. Dvorkin, "Cyber-Physical Resilience of Electrical Power Systems Against Malicious Attacks: a Review," *Current Sustainable/Renewable Energy Reports*, vol. 5, no. 1, pp. 14–22, 2018.

[14] F. Nejabatkhah, Y. W. Li, H. Liang, and R. Reza Ahrabi, "Cyber-security of smart microgrids: A survey," *Energies*, vol. 14, no. 1, 2021.

[15] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[16] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance Attacks on Load Frequency Control of Smart Grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4490–4502, 2018.

[17] S. Chen, T. Zhang, H. B. Gooi, R. D. Masiello, and W. Katzenstein, "Penetration Rate and Effectiveness Studies of Aggregated BESS for Frequency Regulation," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 167–177, 2016.

[18] X. Xie, Y. Guo, B. Wang, Y. Dong, L. Mou, and F. Xue, "Improving AGC Performance of Coal-Fueled Thermal Generators Using Multi-MW Scale BESS: A Practical Application," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1769–1777, 2018.

[19] L. Xing, Y. Mishra, Y.-C. Tian, G. Ledwich, H. Su, C. Peng, and M. Fei, "Dual-Consensus-Based Distributed Frequency Control for Multiple Energy Storage Systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6396–6403, 2019.

[20] A. Levant, "Robust exact differentiation via sliding mode technique," *Automatica*, vol. 34, no. 3, pp. 379–384, 1998.

[21] A. Ferrara, G. P. Incremona, and M. Cucuzzella, *Advanced and Optimization Based Sliding Mode Control: Theory and Applications*. Society for Industrial and Applied Mathematics, 2019.

[22] A. Dev and M. K. Sarkar, "Robust higher order observer based non-linear super twisting load frequency control for multi area power systems via sliding mode," *International Journal of Control, Automation and Systems*, vol. 17, no. 7, pp. 1814–1825, 2019.
[23] G. Rinaldi, M. Cucuzzella, and A. Ferrara, "Sliding mode observers for a network of thermal and hydroelectric power plants," *Automatica*, vol. 98, pp. 51–57, 2018.
[24] C. Mellucci, P. P. Menon, C. Edwards, and A. Ferrara, "Second-order sliding mode observers for fault reconstruction in power networks," *IET Control Theory & Applications*, vol. 11, no. 16, pp. 2772–2782, 2017.
[25] 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.
[26] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1932–1941, 2017.
[27] Q. Su, S. Li, Y. Gao, X. Huang, and J. Li, "Observer-based detection and reconstruction of dynamic load altering attack in smart grid," *Journal of the Franklin Institute*, vol. 358, no. 7, pp. 4013–4027, 2021.
[28] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862–2872, 2016.
[29] B. Stott, J. Jardim, and O. Alsaç, "Dc power flow revisited," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1290–1300, 2009.
[30] G. Bartolini, A. Ferrara, A. Levant, and E. Usai, "On second order sliding mode controllers," in *Variable structure systems, sliding mode and nonlinear control*. Springer, 1999, pp. 329–350.
[31] S. Winder, *Analog and digital filter design*. Elsevier, 2002.
[32] N. P. Bhatia and G. P. Szegö, *Stability theory of dynamical systems*. Springer Science & Business Media, 2002.