On the Optimization of Energy Storage System Placement for Protecting Power Transmission Grids Against Dynamic Load Altering Attacks*

Alessandro Di Giorgio, Alessandro Giuseppi, Francesco Liberati,
Antonio Ornatelli, Antonio Rabezzano, and Lorenzo Ricciardi Celsi

Abstract— **In this paper a power system protection scheme based on energy storage system placement against closed-loop dynamic load altering attacks is proposed. The protection design consists in formulating a non-convex optimization problem, subject to a Lyapunov stability constraint and solved using a two-step iterative procedure. Simulation results confirm the effectiveness of the approach and the potential relevance of using energy storage systems in support of primary frequency regulation services.**

I. Introduction

Over the last years, the need for securing power grids against the danger of cyber-physical attacks has been increasingly encouraging the development of distributed intelligence technologies accompanied by appropriate security enforcements. In particular, cyber-physical attacks have been targeting all sectors of power systems, i.e., generation, distribution and control, and consumption. In this respect, a suitable classification with meaningful examples is given in [1]. More specifically, as concerns cyber-physical attacks targeting the *generation* sector, the interested reader is referred to [2] and [3]; as concerns, instead, cyber-physical attacks targeting the *distribution and control* sector, the reader is referred to [4] and [5].

This paper is focused on cyber-physical attacks targeting the *consumption* sector. In particular, we are concerned with Load Altering Attacks (LAAs) whose aim is to maliciously alter a group of remotely accessible yet unsecured controllable loads, thus artificially creating power imbalances in the power network responsible for frequency and load angle instability, and consequently network blackout through sequential generator tripping.

In particular, LAAs can be classified into *static* ones, which abruptly modify the volume of certain vulnerable loads *una tantum*, and *dynamic* ones (hereafter referred to as D-LAAs), which not only determine the volume of the change enforced onto the compromised load, but also establish the load trajectory over time.

D-LAAs can either be *open-loop* – such that the attacker is not capable of monitoring the power grid in real-time and therefore assigns a pre-programmed trajectory to the compromised load based on some available historical data – or *closed-loop*. Whenever a closed-loop D-LAA is struck against a power grid, the attacker continuously monitors the grid conditions through his own installed sensors or by hacking into an existing monitoring infrastructure, and consequently uses the feedback from the power grid frequency to alter the victim load buses.

Moreover, we distinguish between *single-point* closed-loop D-LAAs, which compromise only the vulnerable load at one victim load bus, and *multi-point* ones, which compromise the vulnerable loads at several victim load buses in a coordinated fashion in order to maximize the attack impact [6]. In this paper, based on the IEEE 39-bus test system, we design a protection scheme against closed-loop single-point and multi-point D-LAAs by formulating and solving a non-convex optimization problem subject to a Lyapunov stability constraint. The paper takes into account the most relevant power system dynamics, and feedback control theory is here used – following approaches similar to those appearing in other papers which apply control-based methodologies to several application fields [7]-[16] – as a tool to model and build a remedy action against the attack: this adds to the already existing results on the control-theoretic study of cyber-physical systems [17][18]. The proposed protection scheme relies upon the proper installation of suitably-sized Energy Storage Systems (ESSs) [19][20] in order to mitigate the effects of the ongoing D-LAA and preserve the power system's stability. In this regard, ESS technology has significantly improved over the last years, with possible applications starting to be investigated at transmission [21][22], distribution [23]-[26], microgrid [27][28] and consumer [29] level. The presented setup is also of practical interest due to its link to the concept of frequency-responsive loads [30][31], which are expected to support traditional power plants in the provisioning of frequency regulation services.

In particular, this study has been carried out within the framework of the H2020 ATENA project, which is aimed at developing ICT networked components for the detection of and reaction to adverse events in the context of cyber-physical security for Critical Infrastructures (CI), where it is crucial to

*Research supported by the European Commission in the framework of the H2020 ATENA project (*Advanced tools to assess and mitigate the criticality of ICT components and their dependencies over critical infrastructures*) under Grant Agreement no. 700581.

A. Di Giorgio, A. Giuseppi, A. Ornatelli, A. Rabezzano, and L. Ricciardi Celsi are with the Department of Computer, Control and Management Engineering Antonio Ruberti, University of Rome La Sapienza, via Ariosto 25, 00185 Rome, Italy (email:{digiorgio, giuseppi, ricciardicelsi}@diag.uniroma1.it).

F. Liberati is with the SMART Engineering Solutions & Technologies (SMARTEST) Research Center, eCampus University, Via Isimbardi 10, 22060 Novedrate (CO), Italy (e-mail: francesco.liberati@uniecampus.it).

prevent the propagation of damage to other CIs interdependent with the power grid (see also the FP7 projects MICIE and CockpitCI [32]-[35] as well as the SHIELD framework and the related publications [36]-[44]). The paper is organized as follows. Section II provides the mathematical model of the IEEE 39-bus test system undergoing a closed-loop D-LAA. Section III formulates the problem of optimizing the number and location of ESSs for protecting the power grid against the ongoing D-LAA. Section IV shows and discusses the performed simulations. Concluding remarks in Section V end the paper.

II. Mathematical Model of the IEEE 39-Bus Test System Under a D-LAA

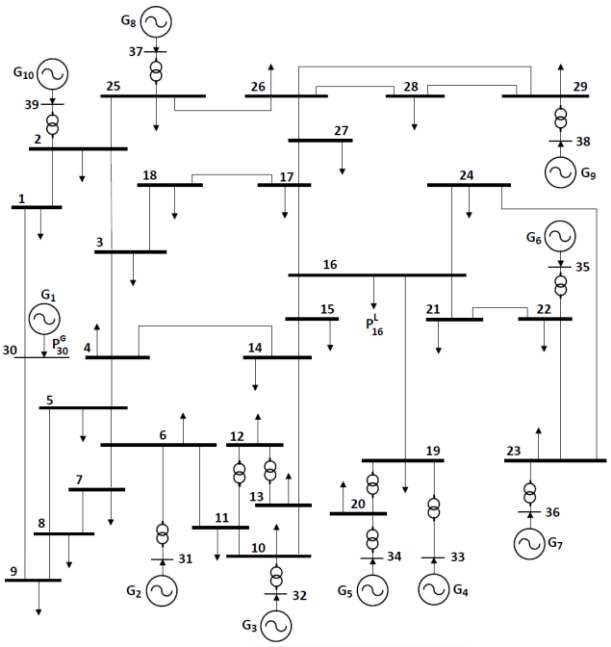

Figure 1. The IEEE 39-bus test system.

We now present the mathematical model for the IEEE 39-bus test system based on the 10-machine New-England power network and depicted in Fig. 1: we will use this model for the design, relying upon ESSs, of a protection scheme against D-LAAs.

Let $\mathcal{G}$ and $\mathcal{L}$ represent the sets of generator buses and load buses, respectively, across the grid. More in detail, the IEEE 39-bus test system is made of 10 generator buses and 29 load buses, so we assume that $\mathcal{L} = \{1, \dots, 29\}$ and $\mathcal{G} = \{30, \dots, 39\}$. Let then $\mathcal{N} = \mathcal{G} \cup \mathcal{L}$ represent the set of all buses across the grid. For a generic bus $i \in \mathcal{N}$, the total amount of power delivered can be separated into generator and load terms [1]. Namely, power flow equations can be written distinguishing the power amount P_i^G injected into the grid by each generator $i \in \mathcal{G}$ and the total power P_i^L absorbed by each load bus $i \in \mathcal{L}$. By defining δ_i as the voltage phase angle of the i-th generator bus, θ_i as the voltage phase angle of the i-th load bus and H_{ij} as the admittance value between the generic i-th and j-th buses, it follows that

$$P_i^G = \sum_{j\in\mathcal{G}} H_{ij}\left(\delta_i - \delta_j\right) + \sum_{j\in\mathcal{L}} H_{ij}(\delta_i - \theta_j), \quad \forall i \in \mathcal{G}$$

$$-P_i^L = \sum_{j\in\mathcal{G}} H_{ij}(\theta_i - \delta_j) + \sum_{j\in\mathcal{L}} H_{ij}(\theta_i - \theta_j), \quad \forall i \in \mathcal{L}. \tag{1}$$

As regards the generator buses, the swing equations are adopted to model the dynamic behavior of each generator $i \in \mathcal{G}$, i.e.,

$$\dot{\delta}_i = \omega_i \tag{2}$$

$$M_i\dot{\omega}_\iota = P_i^M - P_i^G - D_i^G\omega_i, \tag{3}$$

where ω_i is the rotor frequency deviation at the i-th generator bus, M_i is the rotor inertia associated with the i-th generator, P_i^M is the mechanical power input and $D_i^G\omega_i$ is the damping term, proportional to the frequency deviation, $\forall i \in \mathcal{G}$. We assume that the inertia M_i and the damping coefficient D_i^G are strictly positive.

In particular, according to [45] and [46], it is possible to combine a turbine-governor control action with a load-frequency one into a proportional-integral (PI) controller, aimed at keeping the rotor frequency at its nominal level by pushing the frequency deviation ω_i back to zero. Said PI controller is represented by

$$P_i^M = -\left(K_i^P\omega_i + K_i^I\int_0^t \omega_i\right), \quad K_i^P, K_i^I > 0. \tag{4}$$

Consequently, the rotor frequency dynamics in equation (3) can be rewritten by expressing the mechanical power P_i^M for each generator in terms of frequency deviation ω_i, as defined in (4). It follows that

$$M_i\dot{\omega}_i = -\left(K_i^P\omega_i + K_i^I\int_0^t \omega_i\right) - P_i^G - D_i^G\omega_i$$

and, since the power P_i^G injected by the generating unit is defined according to (1) and the integral of the frequency deviation is equal to the voltage phase angle of the generator, we obtain, $\forall i \in \mathcal{G}$,

$$M_i\dot{\omega}_i = -K_i^P\omega_i - K_i^I\delta_i - \\ -\sum_{j\in\mathcal{G}} H_{ij}(\delta_i - \delta_j) - \sum_{j\in\mathcal{L}} H_{ij}(\delta_i - \theta_j) - D_i^G\omega_i.$$

After some manipulations, we have

$$-M_i\dot{\omega}_\iota = (K_i^P + D_i^G)\omega_i + K_i^I\delta_i + \textstyle\sum_{j\in\mathcal{G}} H_{ij}(\delta_i - \delta_j) + \\ \textstyle\sum_{j\in\mathcal{L}} H_{ij}(\delta_i - \theta_j), \quad \forall i \in \mathcal{G}. \tag{5}$$

As regards the load buses, instead, following [31] we use P_i^L to define the aggregate power consumption of (i) uncontrollable loads as well as of (ii) controllable but frequency-insensitive ones. On the other hand, (iii) controllable and frequency-sensitive loads can be assumed to increase linearly with the frequency deviation at the load buses: it follows that the related power consumption can be modeled by $D_i^L\phi_i$, where D_i^L is the strictly positive damping term of the i-th load bus and $\phi_i = -\dot{\theta}_\iota$ is the frequency deviation at each bus $i \in \mathcal{L}$. We can rewrite (1), $\forall i \in \mathcal{L}$, as follows,

$$\dot{\theta}_i = -\phi_i \quad (6)$$

$$-D_i^L\phi_i - P_i^L = \sum_{j\in\mathcal{G}} H_{ij}(\theta_i - \delta_j) + \sum_{j\in\mathcal{L}} H_{ij}(\theta_i - \theta_j). \quad (7)$$

Equations (2), (5), (6), and (7) define the complete dynamical model of the IEEE 39-bus test system depicted in Fig. 1. The power grid can now be represented in the form of a linear state-space descriptor model. First of all, we need to arrange the admittance values, appearing in equations (5) and (7), into four different matrices, that is, (i) H^{GG}, containing the admittance values associated with the lines connecting buses in $\mathcal{G}$; (ii) H^{GL}, containing the admittance values associated with the lines between generator and load buses; (iii) $H^{LG} = (H^{GL})^T$; (iv) H^{LL}, containing the admittance values associated with the lines connecting the buses in $\mathcal{L}$. Therefore, the complete admittance matrix of the power system is

$$H = \begin{bmatrix} H^{GG} & H^{GL} \\ H^{LG} & H^{LL} \end{bmatrix}.$$

Moreover, the inertia and damping values (M_i and D_i^G, respectively) in (5), as well as the damping terms D_i^L in (7), can be collected into properly-dimensioned diagonal matrices, namely M, D^G, and D^L. The same considerations apply to the proportional and integral values K_i^P and K_i^I as well as to the load power consumptions P_i^L. Eventually, by defining $\delta = [\delta_1 \quad \dots \quad \delta_{10}]^T$ as the vector of the voltage phase angles associated with the generators, $\theta = [\theta_1 \quad \dots \quad \theta_{29}]^T$ as the vector of the voltage phase angles associated with the load buses, $\omega = [\omega_1 \quad \dots \quad \omega_{10}]^T$ as the vector of the frequency deviations of the generators, and $\phi = [\phi_1 \quad \dots \quad \phi_{29}]^T$ as the vector of the load frequency deviations, and considering δ, θ, ω, and ϕ as state variables, the complete linear state-space descriptor model for the IEEE 39-bus test system is

$$\begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & -M & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\theta} \\ \dot{\omega} \\ \dot{\phi} \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & -I \\ K^I + H^{GG} & H^{GL} & K^P + D^G & 0 \\ H^{LG} & H^{LL} & 0 & -D^L \end{bmatrix} \begin{bmatrix} \delta \\ \theta \\ \omega \\ \phi \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ I \end{bmatrix} P^L, \quad (8)$$

where the I's are properly-dimensioned identity matrices.

Let us now plug a D-LAA into the system reported above. By definition, a D-LAA is aimed at compromising a certain amount of vulnerable load in specific grid areas and at controlling its evolution over time so that the overall interconnected system is considerably altered and damaged. Therefore, in line with [6], we regard power consumption at the load buses, i.e., P^L, as the sum of two contributions: part of the load consumption is identified as a protected portion P^{LS}, while P^{LV} denotes the vulnerable unprotected portion of the load:

$$P^L = P^{LS} + P^{LV}. \quad (9)$$

Let $\mathcal{V} \subseteq \mathcal{L}$ be the set of victim load buses and let $\mathcal{S} \subseteq \mathcal{N}$ be the set of the positions of sensors which are capable of attack detection. Accordingly, let $K_{vs}^{LG} \geq 0$ denote the attack gain at victim bus $v \in \mathcal{V}$ if the sensor bus s is a generator bus (belonging to $\mathcal{G}$), and $K_{vs'}^{LL} \geq 0$ denote the control gain of the attacker at bus $v \in \mathcal{V}$ if the sensor bus s' is a load bus (belonging to $\mathcal{L}$). A D-LAA against the power grid can then be modelled by the proportional controller

$$P_v^{LV} = -K_{vs}^{LG}\omega_s - K_{vs'}^{LL}\phi_{s'}, \quad (10)$$

where ω_s is the generator frequency deviation measured by a sensor bus $s \in \mathcal{G}$, and $\phi_{s'}$ is the frequency deviation of the load buses measured by a sensor bus $s' \in \mathcal{L}$. In particular, the D-LAA is such that the update of P^{LV} is inversely proportional to frequency deviation: namely, if ω_s decreases (increases), then the amount of vulnerable load increases (decreases), and the same holds with respect to $\phi_{s'}$. Hence, equation (10) is a proportional controller modelling a D-LAA against the power grid. By the way, note that other choices (such as PID or PD controllers) are also possible to model such attacks.

On this basis, the power grid under attack is modelled by substituting (10) into (9), and then into (8), thus obtaining

$$\begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & -M & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\theta} \\ \dot{\omega} \\ \dot{\phi} \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & -I \\ K^I + H^{GG} & H^{GL} & K^P + D^G & 0 \\ H^{LG} & H^{LL} & -K^{LG} & -D^L - K^{LL} \end{bmatrix} \begin{bmatrix} \delta \\ \theta \\ \omega \\ \phi \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ I \end{bmatrix} P^{LS}. \quad (11)$$

When the system is under attack, the attacker can compromise the grid stability by properly modifying the controller gains, and, subsequently, the amount of vulnerable unprotected load P^{LV}. Formally, from a control-theoretic point of view, the closed-loop system above becomes unstable if controller gains K^{LG} and K^{LL} are capable of moving the system poles to the right-hand side of the complex plane, that is, to the unstable region for continuous-time linear systems.

III. Optimization of ESS Placement for Protecting the Power Grid Against a D-LAA

As in [6], the idea is to exploit the notion of Lyapunov stability in combination with an optimization criterion so as to guarantee power grid security in the presence of a D-LAA characterized as in (10). More specifically, in this paper it is proposed to solve the following problem: given a power grid whose load buses are assumed to be potential victims to a D-LAA, determine the minimum number of ESSs (with fixed size) and their exact locations in order to protect the system against the ongoing D-LAA. In this respect, a proper optimization problem can be defined where ESSs are modelled based on feedback from the frequency deviations

detected all across the power grid. Let us assume that the term P^{LS}, that is, the protected portion of the power consumption P^L at the load buses, be the power provided by a certain number of ESSs at different locations in the power grid.

Let us suppose that the sensor bus s is necessarily a generator bus, i.e., $s \in \mathcal{S} \subseteq \mathcal{G}$, and consequently K^{LL} is set to zero. The power provided by an ESS placed at the victim load bus $v \in \mathcal{V}$ can be modelled by a proportional controller in the form

$$P_{vs}^{LS} = K_{vs}^{LS}\omega_s,$$

where $K_{vs}^{LS} \geq 0$ denotes the storage gain at each victim load bus v when the sensor is located at generator bus s and ω_s is the frequency deviation measured at bus s. In other words, we assume that the ESS operating conditions are strictly related to the power grid state and, therefore, to the frequency deviations that occur as a result of the D-LAA being struck against the power grid itself.

Neglecting the $K^{LL}\phi$ term due to the assumption on the sensor bus, the power consumption P^L in (9) can be then rewritten as

$$P^L = (K^{LS} - K^{LG})\omega. \tag{12}$$

The resulting closed-loop system dynamics – modelling the power grid subject to the D-LAA and to ESS control for attack mitigation – is obtained by substituting (12) into (8) so as to have

$$\begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & -M & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\theta} \\ \dot{\omega} \\ \dot{\phi} \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & -I \\ K^I + H^{GG} & H^{GL} & K^P + D^G & 0 \\ H^{LG} & H^{LL} & K^{LS} - K^{LG} & -D^L \end{bmatrix} \begin{bmatrix} \delta \\ \theta \\ \omega \\ \phi \end{bmatrix}.$$

The last row of the descriptor system above can be solved with respect to ϕ and properly substituted in order to obtain an equivalent linear state-space model, i.e.,

$$\begin{bmatrix} \dot{\delta} \\ \dot{\theta} \\ \dot{\omega} \end{bmatrix} = (A - BK) \begin{bmatrix} \delta \\ \theta \\ \omega \end{bmatrix},$$

where

$$A = \begin{bmatrix} 0 & 0 & I \\ -(D^L)^{-1}H^{LG} & -(D^L)^{-1}H^{LL} & 0 \\ -M^{-1}(K^I + H^{GG}) & -M^{-1}(H^{GL}) & -M^{-1}(K^P + D^G) \end{bmatrix},$$

$$B = [0 \quad (D^L)^{-1} \quad 0]^T$$

$$K = [0 \quad 0 \quad K^{LS} - K^{LG}]. \tag{13}$$

At this point, we can formulate the optimization problem. In particular, according to Lyapunov's stability theorem for linear systems, the system poles are required to be kept inside the left-hand side of the complex plane. In this respect, the following linear matrix inequality has to hold if we want to ensure Lyapunov stability, i.e.,

$$(A - BK)^T X + X(A - BK) < 0, \tag{14}$$

with K as in (13), thus implying that the stability of the overall system is strictly related to (i) the entity of the D-LAA against the power grid, and to (ii) the ESS size.

Before formulating the optimization problem, a feasibility constraint on the entity of the D-LAA has to be formulated. Namely, we assume that the attack intensity cannot be greater than the difference between the total vulnerable load at victim load bus v (P_v^L) and the power provided by the corresponding ESS. In other words, the more power the ESSs provide, the less effective the D-LAA against the power grid is.

$$K_{vs}^{LG}\omega_s^{max} \leq \frac{P_v^L - P_v^{LS}}{2} = \frac{P_v^L - K_{vs}^{LS}\omega_s}{2}, \tag{15}$$

where ω_s^{max} denotes the maximum admissible frequency deviation for generator s before its over or under frequency relays trip [6]. Another constraint to be enforced can be expressed in terms of the ESS size. Namely, the storage control gain is limited according to the following relation:

$$K_{vs}^{LS}\omega_s^{max} \leq P_v^{LS,max}, \tag{16}$$

where $P_v^{LS,max}$ is the maximum power provided by the ESS, expressed in p.u. Under these constraints, the optimization problem can be formulated as follows.

Problem 1 (Optimization of number and location of ESSs protecting the power grid against a D-LAA). Given the total vulnerable load P^L at victim load bus $v \in \mathcal{V}$ and given a proper ESS size, determine the minimum number and the exact location of ESSs so that the power grid is asymptotically stable, that is,

$$\min \|K^{LS}\|_0$$

subject to

$$X \succcurlyeq 0,$$

$$X = X^T,$$

Eqs. (14), (15), and (16), $\forall v \in \mathcal{V}$. ■

By minimizing the ℓ_0-norm[1] of vector K^{LS} (i.e., the vector listing all energy storage control gains K_{vs}^{LS} at $v \in \mathcal{V}$ and $s \in \mathcal{S}$), it is possible to determine the minimum number and the optimal location of the ESSs to be installed in the power grid in order to prevent a D-LAA in the form (10) from compromising the overall system stability.

However, note that a solution to this problem is not easily found, because solving a cardinality minimization problem is NP-hard [47], and due to the presence of the non-convex quadratic constraint defined by (15).

For the former problem, an approximation is needed to reduce the computational complexity. A common choice is the minimization of the ℓ_1 norm, characterized by sparse feasible solutions (i.e., solutions which have null elements) [48].

[1] We recall that the ℓ_0-norm of a vector is the number of its non-zero elements, i.e., its cardinality.

Generally, a non-convex optimization problem may have multiple solutions, it may be infeasible or it can take exponential time to determine the global minimum across all admissible solution regions. In order to overtake non-convexity, we exploit a two-step solution approach, adapted from [6] and inspired by the *coordinate descent method* whose convergence is guaranteed [49].

First, note that inequality (15) has to turn into an equality when attempting to solve Problem 1. In fact, if (15) holds as a strict inequality, when the optimal solution is found, one could think of reducing the value of P^{LS} and consequently lower the objective function, thus contradicting the optimality status. It then follows that the constraint in (15) should be rewritten as an equality, making K_{vs}^{LG} act as a slack variable, i.e.,

$$K_{vs}^{LG}\omega_s^{max} = \frac{P_v^L - K_{vs}^{LS}\omega_S}{2} \tag{17}$$

This way, we reduce the decision variables of the optimization problem to K^{LS} and X, since K_{vs}^{LG} is now univocally defined by the vulnerable loads and the power injected by the ESSs. Nevertheless, these two variable sets are still coupled through the attack control gain K_{vs}^{LG} and the non-convex constraint defined by equation (17). To this end, the problem is split up into the two following coupled subproblems.

- Step (1). Initially, the storage control gain vector K^{LS} is assumed to be constant, thus easily determining the attack control gain K_{vs}^{LG} according to constraint (17). This way, we can solve a *feasibility problem* over variable X, i.e.,

  $$\min \|K^{LS}\|_1$$

  subject to

  $$X \succcurlyeq 0,$$
  $$X = X^T,$$
  $$\text{Eqs. (14) and (17)}, \forall v \in \mathcal{V},$$

  where the decision variables are the entries of matrix X. Such a feasibility problem can also be classified as a *semi-definite program* [50].
- Step (2). Next, we take the solution X of the feasibility problem above as a constant and we solve Problem 1 over K^{LS} only, i.e.,

  $$\min \|K^{LS}\|_1$$

  subject to Eqs. (14), (16), and (17), $\forall v \in \mathcal{V}$,

  where the decision variables are the entries of K^{LS}.

These two steps are iterated until convergence is reached. In particular, note that the ESS number and placement is assessed, as a result of the optimization procedure: the non-zero elements of the resulting K^{LS} vector identify the optimal number and location of the ESSs to be deployed.

IV. Simulation Results

The simulations presented in this section have been carried out using MATLAB®: in particular, the authors relied upon the CVX package [51] for determining a numerical solution to Problem 1 according to the two-step iterative procedure explained above. As regards the values of the parameters of the transmission lines, of the inertia (i.e., M) and damping coefficients (i.e., D^G) of generators, of the generator controller gains (i.e., the K_i^P's) and of the damping coefficients for each dynamic load (i.e., the D_i^L's), such values are chosen as in [6]. In particular, the controller parameters are set in order to keep the overall system stable during normal operations, i.e., in the absence of an attack. The nominal system frequency is 60 Hz. We assume that the over-frequency relays of the generators trip at 62 Hz, whereas the under-frequency relays trip at 58 Hz. Consequently, i.e., $\omega_s^{max} = 2/60$. The vulnerable loads at each load bus are reported in Table I. Note that, unlike [6] we are assuming the power loads reported in Table I to be entirely vulnerable. Therefore, in our scenario, the way chosen to protect them is by relying on the power provision allowed by suitably-deployed ESSs.

TABLE I. Vulnerable Loads at each Load Bus (P^L)

Load Bus v	P_v^L (p.u.)	Load Bus v	P_v^L (p.u.)	Load Bus v	P_v^L (p.u.)
1	4	**11**	4	**21**	6.7
2	4	**12**	4.1	**22**	4
3	7.2	**13**	4	**23**	9.8
4	9	**14**	4	**24**	7
5	4	**15**	7.2	**25**	6.2
6	7	**16**	10.9	**26**	5.4
7	6.3	**17**	4	**27**	6.8
8	9.2	**18**	5.6	**28**	6.1
9	4	**19**	5.6	**29**	15.1
10	4	**20**	10.3	**-**	-

A. First Attack Scenario

With respect to the 10-machine New-England power network depicted in Fig. 1, in the first attack scenario we assume that only a subset of vulnerable loads can be regarded as potential victims to a D-LAA. Let us consider as potential victims only the load buses identified by $\mathcal{V} = \{6, 16, 19, 23, 29\}$ and let us assume that the sensor capable of detecting the ongoing attack is located at generator bus $s = 33 \subset \mathcal{G}$. Let us also assume that the vulnerable loads at the victim load buses are $P^L = [7\ 10.9\ 5.6\ 9.8\ 15.1]^T$ and let the ESS size be equal to the available load at the victim load buses. This last assumption implies that the initial values of the storage control gains are set to $P^L/2\omega_s^{max}$.

Starting from control gains initialized to the maximum admissible values, the iterative algorithm discussed in Section III is run so as to solve this instance of Problem 1. Since we intend to determine the minimum number of ESSs and their exact location in the power grid, the obtained simulation results claim that, by introducing one ESS located at load bus no. 19 with storage capacity equal to 5.6 p.u., the power grid remains stable under the considered D-LAA.

B. Second Attack Scenario

In the second attack scenario, we still assume that the sensor detecting the D-LAA is located at generator bus $s = 33$ and that the victim load buses are $\mathcal{V} = \{6, 16, 19, 23, 29\}$. This time, however, we intend to analyze the impact of the ESS size on the optimization problem solution: by contrast with the previous scenario, where the ESS size is fixed and initialized to $P^L/2\omega_s^{max}$, we now consider different sizes and assess how the power provided by the ESSs influences the feasibility of the optimization problem. To this end, we assume that the power provided by the ESSs starts from 1 p.u. The iterative algorithm is run for each different size in order to determine whether the corresponding problem for the determination of the optimal ESS location is solvable. Starting from ESSs with unit size, the problem is solved; then, by increasing the size by one unit at a time, the problem is solved again. Such a procedure is repeated until convergence to a constant number of ESSs is obtained, with no further increase in the number of ESSs as the size grows. In particular, the optimal ESS placement problem turns out to be infeasible for ESS sizes equal to 1 p.u., 2 p.u., and 3 p.u.: indeed, for such values, the iterative algorithm proposed above is not able to determine an admissible solution such that the overall system stays stable under attack. Note that, instead, at 4 p.u., it is possible to determine an exact number of ESSs (i.e., 2) such that the overall system stability is ensured. For sizes of 5 p.u. or greater, just one ESS is sufficient to guarantee stability under the considered D-LAA.

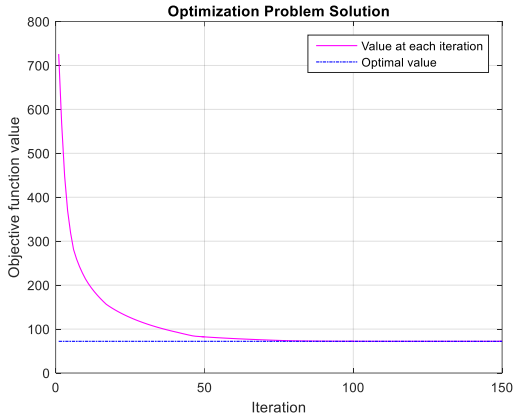

Figure 2. Convergence result of the iterative algorithm solving Problem 1 in the first attack scenario.

V. Conclusion

In this paper a protection scheme making use of energy storage systems for improving power system reaction to closed-loop dynamic load altering attacks is presented. The problem is formulated as a non-convex optimization problem subject to a Lyapunov stability constraint for the autonomous representation of the power system obtained after linearization and application of the attack and frequency control laws. The reported results show how the proposed two-step iterative algorithm allows to determine a solution to the problem of optimizing the number and location of energy storage systems, ensuring grid stability. Yet, the deployability of the resulting solution depends on the availability on the market of suitably-sized energy storage systems.

The authors are currently attempting to tackle the presented problem by means of a greedy method for finding a sparse solution, namely the so-called *matching pursuit* one, with the aim of comparing the related results with those obtained by minimizing the ℓ_1 norm of the storage control gain vector. Moreover, future works will consider the placement of energy storage systems for reducing the possibility of designing undetectable attacks as well as for their usage in support of secondary regulation services. The authors are also carrying out further studies with the aim of applying the methodologies discussed in [52]-[54] to the problem of QoE-aware smart grid protection against cyber-physical attacks.

Acknowledgment

The authors wish to thank Dr. A. Pietrabissa for the fruitful discussions and comments on the paper's content. The authors also gratefully acknowledge the members of the ATENA project and, in particular, the ATENA participants from the Consortium for Research in Automation and Telecommunications (CRAT), Rome, Italy.

References

[1] Pasqualetti, F., Dörfler, F., Bullo, F. "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 110-127, 2015.

[2] W.F. Boyer and S.A. McBride, "Study of security attributes of smart grid systems - current cyber secrity issues," *USDOE*, 2009.

[3] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attacks on electric power systems," in *Power Systems Conference and Exposition, 2009, PSCE'09, IEEE/PES*, IEEE, 2009, pp. 1-8.

[4] Y. Liu, P. Ning, and M.K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, 2011.

[5] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *IEEE International Conference on Smart Grid Communications*, Brussels, Belgium, 2011.

[6] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic Load Altering Attacks against Power System Stability: Attack Models and Protection Designs," *IEEE Trans. on Smart Grid*, in press, 2016.

[7] F. Delli Priscoli, A. Isidori, "A Control-Engineering Approach to Integrated Congestion Control and Scheduling in Wireless Local Area Networks," *Control Engineering Practice*, IFAC (Great Britain), vol. 13, no. 5, May 2005, pp. 541-558.

[8] C. Bruni, F. Delli Priscoli, G. Koch, I. Marchetti, "An Optimal Approach to the Connection Admission Control Problem," *International Journal of Control*, vol. 79, no. 10, October 2006, 1237-1250.

[9] F. Delli Priscoli, F. Di Paolo, A. Fiaschetti, A. Pietrabissa, "A Robust Adaptive Congestion Control for Communication Networks with Time-Varying Delays," *Proceeding of the IEEE Conference on Control Applications*, Munich (Germany), October 4-6, 2006, pp. 2093-2098.

[10] F. Delli Priscoli, A. Pietrabissa, "Control-based Connection Admission Control and Downlink Congestion Control Procedures for Satellite Networks," *Journal of the Franklin Institute*, Elsevier (Great Britain), vol. 346, no. 9, November 2009, pp. 923-944.

[11] C. Bruni, F. Delli Priscoli, G. Koch, I. Marchetti, "Resource Management in Network Dynamics: an Optimal Approach to the Admission Control Problem," *Computers & Mathematics with Applications*, Elsevier, Great Britain, vol. 59, 2010, pp. 305-318.

[12] S. Canale, F. Delli Priscoli, A. Di Giorgio, A. Lanna, A. Mercurio, M. Panfili, V. Suraci, "Resilient Planning of PowerLine Communications Networks Over Medium Voltage Distribution Grids," *20th Mediterranean Conference on Control and Automation (MED12)*, Barcelona (Spain), July 2012, pp. 710-715.

[13] C. Bruni, F. Delli Priscoli, G. Koch, A. Pietrabissa, L. Pimpinella, "Network Decomposition and Optimal Multipath Routing Control Problem for Load Balancing," *Transactions on Emerging*

Telecommunications Technologies (ETT), John Wiley & Sons, Inc., USA, vol. 24, no. 2, March 2013, pp. 154-165.

[14] S. Battilotti, C. Gori Giorgi, S. Monaco, M. Panfili, A. Pietrabissa, L. Ricciardi Celsi, and V. Suraci, "A Multi-Agent Reinforcement Learning Based Approach to Quality of Experience Control in Future Internet Networks," in *Proc. of the 34th Chinese Control Conference (CCC2015)*, pp. 6495-6500, DOI: 10:1109/ChiCC.2015.7260662.

[15] S. Canale, et al., "A Future Internet oriented user centric extended intelligent transportation system," in *Proc. of the 2016 24th Mediterranean Conference on Control and Automation (MED)*, Athens, 2016, pp. 1133-1139. DOI: 10.1109/MED.2016.7535967.

[16] F. Cimorelli, F. Delli Priscoli, A. Pietrabissa, L. Ricciardi Celsi, V. Suraci, and L. Zuccaro, "A Distributed Load Balancing Algorithm for the Control Plane in Software Defined Networking," in *Proc. of the 24th Mediterranean Conference on Control and Automation (MED 2016)*, pp. 1033-1040, DOI: 10.1109/MED.2016.7535946.

[17] F. Pasqualetti, A. Bicchi, and F. Bullo, "A graph-theoretical characterization of power network vulnerabilities," in *Proc. Of the IEEE American Control Conference*, San Francisco, CA, 2011.

[18] 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.

[19] M.C. Falvo, L. Martirano, D. Sbordone and E. Bocci, "Technologies for smart grids: A brief review," *2013 12th International Conference on Environment and Electrical Engineering*, Wroclaw, 2013, pp. 369-375. doi: 10.1109/EEEIC.2013.6549544.

[20] M. Barbetta, M.C. Falvo, C. D'Adamo, L. D'Orazio and E. Duca, "Energy storage systems and distribution grids: A real case study in Italy," *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC*), doi: 10.1109/EEEIC.2016.7555881.

[21] D. Gayme and U. Topcu, "Optimal power flow with large-scale storage integration," *Power Systems, IEEE Transactions on*, 28(2):709–717, May 2013.

[22] A. Di Giorgio, F. Liberati, A. Lanna, "Real Time Optimal Power Flow integrating Large Scale Storage Devices and Wind Generation", *23rd Mediterranean Conference on Control and Automation, MED15, IEEE*, pp.480-486, 2015, DOI: 10.1109/MED.2015.7158794.

[23] S. Manfredi, M. Pagano, R. Raimo, "Ultracapacitor-based Distributed Energy Resources to support time-varying smart-grid power flows," in *Proc. International Symposium IEEE Speedam 2012*. vol. 1, p. 1148-1153, IEEE, ISBN: 9781467313001, Sorrento (Italy), June 2012.

[24] A. Di Giorgio, F. Liberati, A. Lanna, "Electric Energy Storage Systems Integration in Distribution Grids," *IEEE International Conference on Environment and Electrical Engineering, EEEIC15*, 1279-1284, 2015, DOI: 10.1109/EEEIC.2015.7165354.

[25] A. Di Giorgio, F. Liberati, A. Lanna, A. Pietrabissa, F. Delli Priscoli, "Model Predictive Control of Energy Storage Systems for Power Tracking and Shaving in Distribution Grids", *IEEE Transactions on Sustainable Energy*, IEEE, 2016, ISSN: 1949-3029.

[26] A. Nagarajan and R. Ayyanar, "Design and strategy for the deployment of energy storage systems in a distribution feeder with penetration of renewable resources," *IEEE Transactions on Sustainable Energy*, 2015.

[27] Y. Levron, J.M. Guerrero, and Y. Beck, "Optimal power flow in microgrids with energy storage," *Power Systems, IEEE Transactions on*, 28(3): 3226–3234, Aug 2013.

[28] A. Di Giorgio, F. Liberati, R. Germanà, M. Presciuttini, L. Ricciardi Celsi, and F. Delli Priscoli, "On the Control of Energy Storage Systems for Electric Vehicles Fast Charging in Service Areas," in *Proceedings of the 24th Mediterranean Conference on Control and Automation (MED 2016)*, pp. 955-960, DOI: 10.1109/MED.2016.7535947.

[29] A. Di Giorgio, L. Pimpinella, F. Liberati, "A model predictive control approach to the load shifting problem in a household equipped with an energy storage unit", *20th Mediterranean Conference on Control and Automation MED12,* 1491-1498, DOI: 10.1109/MED.2012.6265850.

[30] A. Molina-Garcia, F. Bouffard, and D.S. Kirschen, "Decentralized demand-side contribution to primary frequency control," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 411-419, 2011.

[31] C. Zhao, U. Topcu, and S.H. Low, "Optimal load control via frequency measurement and neighborhood area communication," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 3576-3587, 2013.

[32] F. Caldeira, et al., "Secure mediation gateway architecture enabling the communication among critical infrastructures," *Future Network and Mobile Summit*, IEEE, 2010.

[33] P. Capodieci, R. Setola, F. Delli Priscoli, M. Castrucci, V. Suraci et al., "Improving Resilience of Interdependent Critical Infrasructures via on-line Alerting System," *Complexity in Engineering Conf. (Compeng 2010)*, Rome, pp. 88-90, December 2010.

[34] A. Di Giorgio, F. Liberati, "Interdependency modeling and analysis of critical infrastructures based on Dynamic Bayesian Networks," *19th Mediterranean Conference on Control and Automation MED11*, IEEE, 791–797, Corfu, June 2011, DOI: 10.1109/MED.2011.5983016.

[35] A. Di Giorgio, F. Liberati, "A Bayesian Network-Based Approach to the Critical Infrastructure Interdependencies Analysis," *IEEE Systems Journal*, Special Issue "Complexity in Engineering: from Complex Systems Science to Complex Systems Technology", 6(3), pp. 510-519, 2012, DOI: 10.1109/JSYST.2012.2190695.

[36] F. Caldeira, M. Castrucci, M. Aubigny, D. Macone, E. Monteiro, R. Simoes, V. Suraci, "Secure Mediation Gateway Architecture Enabling the Communication Among Critical Infrastructures," *Future Network and MobileSummit 2010*, ISBN: 978-1-905824-16-8.

[37] A. Fiaschetti, F. Lavorato, V. Suraci, A. Palo, A. Taglialatela, A. Morgagni, A. Baldelli, F. Flammini, "On the use of semantic technologies to model and control Security, Privacy and Dependability in complex systems," *Proc. Of 30th International Conference on. Computer Safety, Reliability and Security (SAFECOMP'11)*, Sep. 2011. Naples, Italy, Doi: 10.1007/978-3-642-24270-0_34.

[38] F. Delli Priscoli, A. Fiaschetti, V. Suraci, "The SHIELD Framework: how to control Security, Privacy and Dependability in Complex Systems," *2012 IEEE Workshop on Complexity in Engineering*, Doi: 2-s2.0-84866534292.

[39] V. Suraci, A. Fiaschetti, "Design and implementation of a service discovery and composition framework for security, privacy and dependability control," *Future Network & Mobile Summit 2012 Conference Proceedings*.

[40] V. Suraci, A. Marucci, R. Bedini, L. Zuccaro, A. Palo, "Energy-aware control of home networks", *Lecture Notes in Computer Science* (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 7972 LNCS (Part 2), pp. 299-311, 2013, Doi: 10.1007/978-3-642-39643-4_23.

[41] R. Pecori, L. Veltri, "Trust-based routing for Kademlia in a sybil scenario," *22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Doi: 10.1109/SOFTCOM.2014.7039131.

[42] R. Pecori, "S-Kademlia: A trust and reputation method to mitigate a Sybil attack in Kademlia," *Computer Networks*, Doi: 10.1016/j.comnet.2015.11.010.

[43] R. Pecori, "A comparison analysis of trust-adaptive approaches to deliver signed public keys in P2P systems," *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*, Doi: 0.1109/NTMS.2015.7266463.

[44] A. Merlo, M. Migliardi, L. Caviglione, "A Survey on Energy-Aware Security Mechanisms," *Pervasive & Mobile Computing*, vol. 24, pp. 77-90, Dec. 2015, Elsevier. DOI:10.1016/j.pmcj.2015.05.005.

[45] J.D.D. Glover and M. S. Sarma, *Power System Analysis and Design*. Brooks/Cole Publishing Co., Pacific Grove, CA, USA, 3rd edition, 2001.

[46] J.D.D. Glover, M. S. Sarma, and T. J. Overbye, *Power System Analysis and Design*. 5th ed. Cengage Learning, 2009.

[47] B. K. Natarajan, "Sparse Approximate Solutions to Linear Systems," *SIAM Journal on Computing*, vol. 24, no. 2, pp. 227-234, 1995.

[48] I. Rish and G. Grabarnik, *Sparse Modeling: Theory, Algorithms, and Applications*, CRC Press, 2014.

[49] D.P. Bertsekas and J.N. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods*. Prentice-Hall, Inc., 1989.

[50] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, New York, NY, USA, 2004.

[51] S. Boyd, M. Grant, *CVX: Matlab Software for Disciplined Convex Programming*, version 2.1, http://cvxr.com/cvx/

[52] F. Delli Priscoli, M. Iannone, A. Pietrabissa, V. Suraci, "Modelling Quality of Experience in Future Internet Networks," *Future Network & Mobile Summit 2012,* Berlin, July 2012.

[53] C. Bruni, F. Delli Priscoli, G. Koch, A. Palo, A. Pietrabissa, "Quality of Experience Provision in the Future Internet," *IEEE Systems Journal,* vol. 10, no. 1, March 2016, pp. 302-312.

[54] F. Delli Priscoli, A. Di Giorgio, F. Lisi, S. Monaco, A. Pietrabissa, L. Ricciardi Celsi, V. Suraci, "Multi-Agent Quality of Experience Control," *International Journal of Control, Automation, and Systems*, vol. 15, no. 2, pp. 892-904, 2017, Doi: 10.1007/s12555-015-0465-5.