Ensuring the Stability of Power Systems Against Dynamic Load Altering Attacks: A Robust Control Scheme Using Energy Storage Systems

Roberto Germanà, Alessandro Giuseppi*, Alessandro Di Giorgio

***Abstract*— This paper presents a robust protection scheme to protect the power transmission network against a class of feedback-based attacks referred in the literature as "Dynamic Load Altering Attacks" (D-LAAs). The proposed scheme envisages the usage of Energy Storage Systems (ESSs) to avoid the destabilising effects that a malicious state feedback has on the power network generators. The methodologies utilised are based on results from polytopic uncertain systems, invariance theory and Lyapunov arguments. Numerical simulations on a test scenario validate the proposed approach.**

Keywords: Dynamic Load Altering Attacks, Electric Energy Storage Systems, Robust Control

NOMENCLATURE

δ	Voltage phase angle at generator buses
ω	Frequency deviation at generator buses
ϕ	Frequency deviation at load buses
M	Inertia matrix of the generators
n, m	number of generators and load buses
$\mathcal{M}_a, \mathcal{M}_p$	sets of vulnerable and secure buses
D, D^L	Damping coefficient matrices
P^L	Power consumption at load buses
K^P, K^I	Generator controller gain matrices
K^{LG}	Attack gain matrix
α	Decrease rate of the Lyapunov function
u_{max}	Bound on the ESS power norm
$\mathbf{0}_n, \mathbf{1}_n$	Column vectors of zeros and ones of size n

I. INTRODUCTION

Energy storage systems (ESSs) are becoming an integral part of modern power networks. In fact, the flexibility offered by their capability to absorb or release power in a controlled way proved to be a promising enabler for the provisioning of ancillary services aimed at improving power quality and voltage stability performances [1], while also contributing to optimal renewable sources usage [2], [3]. It was expected then that, due to the ever increasing penetration of distributed renewable energy sources and electro-mobility [4], ESSs research and number has significantly increased in the last few years.

Devices such as ESSs, controllable loads and distributed generators require for their functioning complex control systems together with information gathered from several heterogeneous sources, as market signals and remote network state measurements. As a consequence, power systems as a whole have evolved towards highly interconnected cyber-physical systems in which a modern ICT control system manages the dynamics and operational constraints of the physical network [5]. Treating power networks as active cyber-physical systems offers significant improvements in their economic performances, enabling functionalities such as dynamic exploitation of power tariffs and demand side management programs [6], but at the same time, due to the interconnected nature of the modern ICT control systems, introduces also several new vulnerabilities in the network [7].

Among the various cyber attacks that target power networks, this work focuses on the so-called "Dynamic Load Altering Attacks" (D-LAAs), originally presented in [8]. D-LAAs are feedback-based attacks that aim at destabilising the transmission network by dynamically controlling, in a malicious way, compromised flexible loads that could be normally used for demand side management programs or smart functionalities.

This paper presents a protection scheme based on robust control methods and Lyapunov arguments to protect power networks against D-LAAs by controlling ESSs in such a way that the destabilising effects of D-LAAs are compensated without requiring any real-time detection or reconstruction of the attack. With respect to the previous work from the authors [9], developed in the scope of the H2020 ATENA project [10], this paper proposes a defence strategy that has robust properties against a whole set of identified potential D-LAAs whereas [9] assumed the attack characteristics to be known. This paper also differentiates from [11] as the protection scheme proposed by its authors was based mainly on securing loads, and consequently reducing the degree of freedom available to the attacker, while this work proposes a control law for an active component of the grid namely ESSs, without affecting the attacker capabilities.

The main contributions and the distinctive features of this work are:

i) The characterisation of the systems subject to D-LAA as polytopic uncertain systems, whose dynamics potentially switch over time depending on the attack.
ii) The development of a control strategy, based on results from robust control theory and invariance arguments, of a robust protection scheme that ensures the asymptotic network stability against the considered set of D-LAAs.
iii) The introduction of an optimisation framework with which the network operators may tune the performance

* corresponding author

This work is partially supported by the SAPIENZA - ATENEO 2017 "PROMETEO - Protezione di reti elettriche di potenza da attacchi ciber-fisici mediante strategie di controllo" project, no. RM11715C7EFAF857.

R. Germanà, A. Giuseppi and A. Di Giorgio are with the Department of Computer, Control, and Management Engineering Antonio Ruberti at Sapienza University of Rome, Via Ariosto, 25, 00185 Rome, Italy, e-mail: {germana,giuseppi,digiorgio}@diag.uniroma1.it.

and characteristics of the control law that manages the ESSs.

The objective of the proposed control law is to assure the asymptotic stability of the network subject to D-LAAs which are taken into account as a form of parametric uncertainty. It will be shown that the resulting system takes the form of a polytopic uncertain linear system with time switching dynamics, and consequently the control law will be designed in such a way that, over the whole range of uncertain and switching dynamics, the Lyapunov inequality holds and the control effort is bounded.

The rest of the paper is structured as follows: Section II reports some required preliminary notions; Section III details the network and attack models, as well as the proposed control logic; Section IV presents some numerical simulation results to validate the proposed approach while Section V draws the conclusions and highlights possible future works.

II. Preliminaries

This section reports some useful definitions and results that are required in the following analysis.

Definition 1: A Polytopic Linear Differential Inclusion (LDI) system is defined as [12]:

$$\dot{x} = A(\zeta)x + B(\zeta)u, \tag{1}$$

where

$$\zeta \in Z = \{[\zeta_1, \zeta_2, ..., \zeta_p]^T \mid \zeta_i \geq 0 \quad \forall i \ \in [1, p], \ \sum_{i=1}^{p} \zeta_i = 1\} \tag{2}$$

models the system uncertainties and the matrices $A(\zeta), B(\zeta)$ are elements of the convex hull of a finite set of known "vertex" matrices $A_i, B_i, i \in [1, p]$, i.e.:

$$A(\zeta) = \sum_{i=1}^{p} \zeta_i A_i, \tag{3}$$
$$B(\zeta) = \sum_{i=1}^{p} \zeta_i B_i.$$

Definition 2: A Linear Time Invariant Switched Systems with arbitrary switching signal $\phi(t) : \mathbb{R}^+ \rightarrow S = \{1, 2, ..., s\}$ is defined as a system of the form [13], [14]:

$$\begin{aligned} \dot{x} &= A_i x + B_i u \\ i &= \phi(t). \end{aligned} \tag{4}$$

When modelling an uncertain system as a polytopic LDI system, one possible approach to study its asymptotic stability is related to the existence of a so-called "Common" Lyapunov Function [15]. In fact, to assure the asymptotic stability of a system of the form (4) under a state feedback $u = Kx$, it is sufficient to prove that, for any symmetric matrix $Q > 0$, there exist a single symmetric matrix $P > 0$ such that:

$$(A(\zeta) + B(\zeta)K)^T P + P(A(\zeta) + B(\zeta)K) = -Q, \forall \zeta \in Z, \tag{5}$$

which, due to the polytopic nature of the matrix uncertainties, is equalent to the existance of a symmetric matrix $P > 0$ that satisfies:

$$(A_i + B_i K)^T P + P(A_i + B_i K) < 0, \ \forall i \in [1, p]. \tag{6}$$

Furthermore, it is worth remarking that Common Quadratic Lyapunov Functions (CQLFs) are also typically used to prove the quadratic, and hence asymptotic, stability of switched systems of the form (4) with analogous arguments and conditions of the ones reported above [13].
Quadratic stability and stabilizability of switched linear systems with polytopic uncertainties under state feedback has received a considerable amount of attention [16]–[18]. In general, the existence of a CQLF is only sufficient for the asymptotic stability and could hence be rather conservative, but the algebraic conditions required to assure the existence of a CQLF for the switched system considered can not be trivially derived [19]. In the following, we will resort to numerical analysis to evaluate the existence of a CQLF for the system and the consequent feasibility of the related optimisat ion problem.

Definition 3: Given a symmetric matrix $P > 0$, the ellipsoid

$$\mathcal{E}(P) = \{x \in \mathbb{R}^n : x^T P^{-1} x \leq 1\} \tag{7}$$

centered at the origin of a linear system is said to be *invariant attractive* [20] for the closed loop system

$$\dot{x} = (A + BK)x \tag{8}$$

if for any $x_0 \in \mathcal{E}(P)$ the evolution of the system remains in $\mathcal{E}(P)$ and ultimately tends to the origin.
In this work the following theorem from [20] will be utilised:

Theorem 1: Let P, Y be solution of following semidefinite programming problem:

$$\begin{gathered} \max tr(P) \\ s.t. \\ \begin{bmatrix} AP + PA^T + BY + Y^T B^T & P \\ P & -I/\alpha \end{bmatrix} < 0 \\ \\ \begin{bmatrix} P & Y^T \\ Y & u_{max}^2 I \end{bmatrix} \geq 0 \end{gathered} \tag{9}$$

in the matrix variables $P = P^T$ and Y, with $\alpha > 0$. Then:

i) the control $u = Kx$, where $K = YP^{-1}$ asymptotically stabilizes the system (8),
ii) u is bounded on the ellipsoid $\mathcal{E}(P)$ so that $||u|| \leq u_{max}$,
iii) $V(x) = x^T P^{-1} x$ is a Lyapunov function for (8)
iv) the ellipsoid $\mathcal{E}(P)$ is the one that maximises the sum of its squared semiaxes among all the invariant ellipsoids of the system (8) over which $V(x)$ decreases not slower than $-\alpha \ ||x||^2$.

III. Problem Formulation

A. Network Model

The transmission network is modelled as in [11], utilising the linearized swing and power flow equations [21]. Let the network be composed by n generator buses and m load buses, of which m_a are vulnerable to a D-LAA and m_p are considered secure and candidate placement option for ESSs. In the following, $\mathcal{M}_a$ and $\mathcal{M}_p$ will represent respectively the set of vulnerable and secured load buses.

The dynamics of the system are captured by the following descriptor system:

$$\begin{bmatrix} I & 0 & 0 & 0 \\ 0 & M & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \\ \dot{\theta} \\ \dot{\phi} \end{bmatrix} = - \begin{bmatrix} 0 & -I & 0 & 0 \\ L_{gg} + K^I & D + K^P & L_{gl} & 0 \\ 0 & 0 & 0 & I \\ L_{lg} & 0 & L_{ll} & -D^L \end{bmatrix} \begin{bmatrix} \delta \\ \omega \\ \theta \\ \phi \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ P^L \end{bmatrix}, \tag{10}$$

in which $M = diag(M_1, \ldots, M_n)$ is the inertia matrix of the generators, K^P and K^I capture respectively the proportional and integral control actions of the generators and D^L the self-regulating effect of the load. The matrix

$$L = \begin{bmatrix} L_{gg} & L_{gl} \\ L_{lg} & L_{ll} \end{bmatrix} \tag{11}$$

is the laplacian of the network [22]. Note that in the considered scenario $L_{gg} \in \mathbb{R}^{n \times n}$, $L_{gl} \in \mathbb{R}^{n \times m}$, $L_{lg} \in \mathbb{R}^{m \times n}$ and $L_{ll} \in \mathbb{R}^{m \times m}$.

B. Attack Model

The structure of the attack considered in this work is derived from [11], where D-LAA are driven by a proportional controller with time varying gain. Assuming that the attack is launched on the load bus $v \in \mathcal{M}_a$ starting from the measure of the electrical frequency deviation of the generator s, the attack takes the form:

$$P_v^{LV}(t) = -K_{vs}^{LG}(t)\omega_s(t). \tag{12}$$

It can be shown with simple mathematical manipulation reported in [11], that the attack can be included in the dynamics of the network (10). Proceeding as in [11] by including the power flow equations in the swing equations, the descriptor system (10) becomes explicitable and it can be reconducted to the linear system

$$\begin{bmatrix} \dot{\delta} \\ \dot{\theta} \\ \dot{\omega} \end{bmatrix} = \begin{bmatrix} 0 & 0 & I \\ (-D^L)^{-1}L_{lg} & (-D^L)^{-1}L_{ll} & (-D^L)^{-1}K^{LG} \\ M^{-1}(L_{gg} + K^I) & M^{-1}L_{gl} & M^{-1}(D + K^P) \end{bmatrix} \begin{bmatrix} \delta \\ \theta \\ \omega \end{bmatrix} + - \begin{bmatrix} 0 \\ (-D^L)^{-1} \\ 0 \end{bmatrix} u. \tag{13}$$

Note that the presence of attacks is included in the system (13) by the term $(-D^L)^{-1}K^{LG}$. In this representation, the overall attack can be seen as a form of parametric uncertainty, as the dynamical matrix of system (13) can be written in the following form:

$$A = \begin{bmatrix} 0 & 0 & I \\ (-D^L)^{-1}L_{lg} & (-D^L)^{-1}L_{ll} & 0 \\ M^{-1}(L_{gg} + K^I) & M^{-1}L_{gl} & M^{-1}(D + K^P) \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & (-D^L)^{-1}K^{LG} \\ 0 & 0 & 0 \end{bmatrix}. \tag{14}$$

It is worth noting that the matrix K^{LG} is a sparse matrix whose non-zero elements K_{vs}^{LG} represent the gains of the ongoing attacks of the form (12). It is then possible to define an uncertainty range, as the various K_{vs}^{LG} that characterise every possible attack are bounded as in [11] by the amount of vulnerable load available on the node $v \in \mathcal{M}_a$, and by the availability of the measure of the frequency deviation at the generator node s. Due to the structure of (14), all possible uncertain dynamical matrices of system (13) lie in the compact set that is obtained by the product of the compact sets over which the various gains of the potential D-LAAs range. The convex hull of such set can be easily characterised by its vertices, as each vertex represent a distinct combination of the various possible D-LAAs each of which taken with its maximum gain K_{vs}^{LG}. Since all possible D-LAAs can be written as a convex combination of these vertices, it follows that the system (13) can be seen as a Polytopic Linear Differential Inclusion system of form (3). Note that if we also include in the analysis the ability of the attacker to modify in real time the gains that define the D-LAA, the network dynamics will switch between matrices that are included in the same polytope.

C. Protection Scheme

We now introduce the following optimisation problem:

$$\begin{aligned} \max_{P,Y,\alpha,\bar{u}_{max}} \quad & \gamma_1 \; tr(P) - \gamma_2 \; \bar{u}_{max} \; + \; \gamma_3 \; \alpha \\ \text{s. t.} \quad & \forall i = 1, ..., p \\ & \begin{bmatrix} A_i P + P A_i^T + BY + Y^T B^T & P \\ P & -I/\alpha \end{bmatrix} \leq 0 \\ & \begin{bmatrix} P & Y^T \\ Y & \bar{u}_{max} I \end{bmatrix} \geq 0 \\ & P = P^T, \end{aligned} \tag{15}$$

where $\gamma_1, \gamma_2, \gamma_3$ represent the relative weights that their corresponding objectives have in the optimisation being the size the ellipsoid, the control saturation and its stabilising performances. In (15) it was set $\bar{u}_{max} = u_{max}^2$ to avoid increasing the complexity of the problem by maintaining the linear nature of its constraints and objective function.

In light of Theorem 1, the function $V(x) = xP^{-1}x$ is a CQLF for all the systems whose dynamics are represented by the vertices $(A_i + BYP^{-1})$ of (13). It follows that the feedback $u = YP^{-1}x$ will asymptotically stabilize the network under attack, independently of which attack is being performed. Additionally, u will be bounded in norm by u_{max}

over the ellipsoid $\mathcal{E}(P)$, where $V(x)$ will decrease with a rate not slower than $-\alpha||x||^2$.

In what was presented so far, it was implicitly assumed u to be unbounded. This assumption is in general unreasonable, as the control effort provided by the available ESSs is limited by their operative power limits. Furthermore, the matrix $K = YP^{-1}$ is in principle dense, meaning that a portion of the control effort (i.e. stabilising power) could be distributed on every load bus. In realistic scenarios the number and location of ESSs to be placed in the network will be limited to a few units and specific, secured, buses previously identified with the set $\mathcal{M}_p$. The details on how both of these limitations are addressed are presented in the following.

Recalling that $\mathcal{M}_p$ was defined as the set of secure buses available for the installation of ESSs, and noting that the presence of a row of zeros in the matrix Y translates by construction to the matrix K, it is possible to restrict the number and locations of the ESSs by adding to (15) a set of constraints that forces the rows of the matrix Y corresponding to buses not contained in $\mathcal{M}_p$ to be formed by zeros. Doing this guarantees that the corresponding elements of the control vector u are identically zero, and hence no ESSs shall be placed on such buses.

Regarding the control saturation, recall that Theorem 1 states that over the invariant ellipsoid the inequality $||u|| \leq u_{max}$ holds. Having a bound on the norm of the control relates to having a limited amount of installed ESS power, and consequently u_{max} can be used as an indicator for the sizing of the distributed storages. In fact, to avoid power outages the network state shall never leave its region of safe operation $\mathbb{X}^S$, as a frequency deviation higher than an operative bound would cause the security mechanisms to stop the service provision. Ideally, the network operator would desire to have the invariant ellipsoid over which the CQLF decreases with its desired rated to be enclosed by $\mathbb{X}^S$, so that the system evolutions are guaranteed to remain in its safe region. On the contrary, attacks that start from initial conditions in $\mathbb{X}^S$ but outside the ellipsoid would be successful in driving the system to instability, as the control effort would saturate.

Furthermore, having a larger invariant ellipsoid implies either worse transient performances or a higher maximum control effort (i.e. larger ESSs), while having a smaller ellipsoid may restrict too much the region of attraction in which the system is robustly stable. Recalling the multi-objective nature of the problem (15), the operator may iterativevly tune the weights $\gamma_1, \gamma_2, \gamma_3$ to attain a ESSs control configuration that satisfies its requirements. Additionally, the network operator may fix any of the three variables that appear in the objective function of (15) (e.g. in scenarios in which the installed ESSs power is predetermined) and run the optimisation to derive the robust control law, in compliance with its use case limitations.

Future research will cover automatic parameter tuning, by means of analytical analysis of the system stable and operative regions characteristics. In fact, a crucial aspect for usage on real scenarios is a proper, and direct, way of mapping the operative requirements of the operator onto the design parameters of the controller.

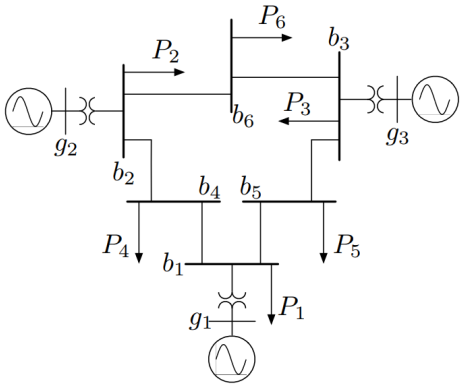

Fig. 1. Transmission network with 6 load buses and three generators

Remark 1: The proposed control scheme protects the network also against D-LAAs in which the attacker changes the exploited load buses, or attack charateristics, over time. In fact, such attacks can be seen as switching the dynamics of the network in the sense of definition 2. Noting that the dynamical matrix (14) switches between matrices that are contained in the polytope characterised by the vertices over which $V(x) = xP^{-1}x$ is a CQLF, from standard switched system arguments it follows that the stability properties of the closed loop system are maintained.

IV. Scenario and simulations

A. Simulation Set Up

For the validation of the proposed control strategy we considered the classical nine-bus example adopted by [23] and reported in Figure 1. We assume that the set of secure loads buses that can host storage is $\mathcal{M}_p = \{5, 6\}$. Additionally, the set of attacks against which the network operator wants to ensure stability is described by a sparse matrix K^{LG} whose non-zero elements have the following indices: $\{(1,2),(2,3),(4,3)\}$. We consider, without loss of generality, the same upper bound for each attack gain, namely 10^6. The weights $\gamma_1, \gamma_2, \gamma_3$ were set respectively to $2, 1, 10$.

B. Baseline Scenario: Destabilising Dynamic Load Altering Attack with no protection

We now proceed to show that the considered D-LAAs are in fact able to destabilise the unprotected power network. Figure 2 shows that a single attack of the form (12) deployed on the load bus 1 starting from the measure of the electrical frequency deviation at generator bus 2 is able to destabilise the network in less than half a second. The fourth subplot of Figure 2 represents how the D-LAA gain varies over time, as a percentage of the maximum consider attack gain.

C. Simulation 1: Defence Against a Single D-LAA

In this simulation, it is shown how the proposed control scheme prevents the destabilising effects of the same D-

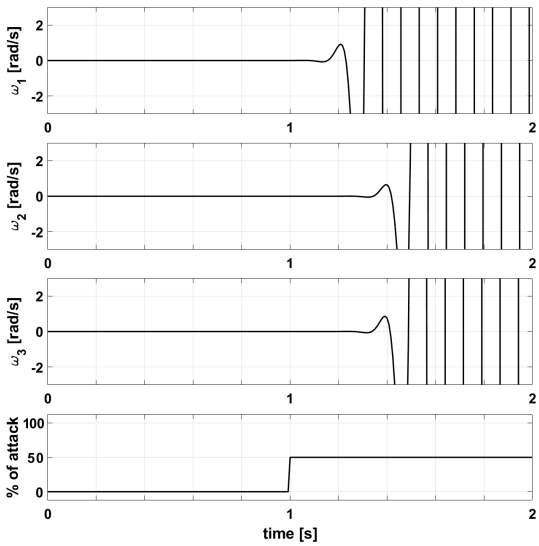

Fig. 2. Frequency deviation for the three generators and attack profile, baseline scenario

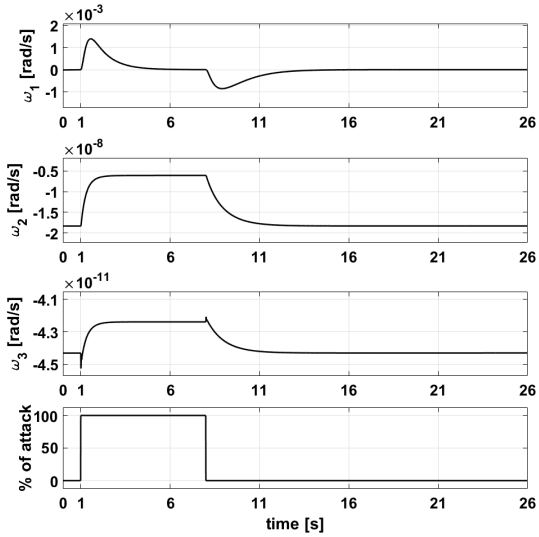

Fig. 3. Frequency deviation for the three generators and attack profile, first simulation

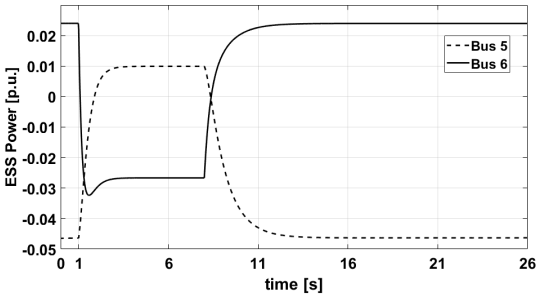

Fig. 4. ESS power profiles, first simulation

LAA of the previous simulation, amplified by a factor of two. From the analysis of the first subplot in Figure 3 it is clear how the switch of the system dynamics caused by the attack starting at $t = 1s$ causes a fluctuation in the first

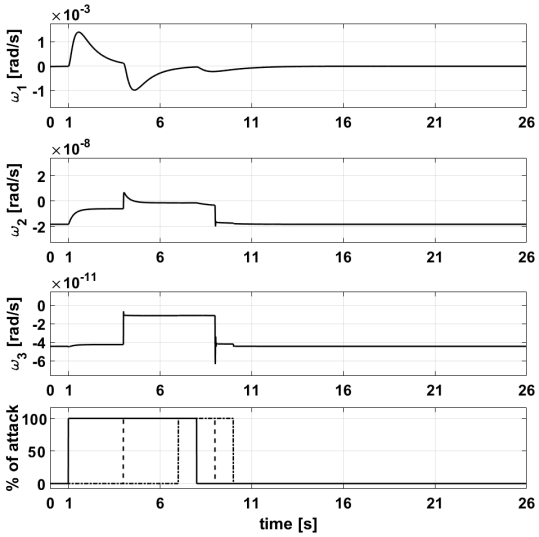

Fig. 5. Frequency deviation for the three generators and attack profile, second simulation

generator frequency, but the effect of the ESSs control avoids that this fluctuation drives the closed loop attacks to steer the network into instability. In fact, the other two generators are almost unaffected by the attack as their frequency deviations are several orders of magnitude lower. It is worth noting how the network recovers after the second switch of its dynamics, caused by the abrupt interruption of the attack at $t = 8s$, with an exponential behaviour. Figure 4 shows the control effort in p.u., and highlights how the actuated control is very limited in magnitude. From the analysis of the figure it is clear how the attack is compensated by the ESSs, as for both the storages their power profile changes sign during the attack. The small magnitude of the defence control is caused ny the fact that the control shares the same state-feedback nature of the attack (12), meaning that around the origin of the system it will be limited: by preventing the D-LAA to steer the system towards the border of its operative region, the control prevents the attack to grow in magnitude. Nevertheless, it is still important to tune both the invariant ellipsoid size and the parameter u_{max} in order to assure that all the operative region is robustly stable, as if the system trajectory starts from an initial state having high frequency deviations both the attack and the stabilising control will be of greater magnitude.

D. Simulation 2: Defence Against Multiple Switching D-LAA

In this final simulation we consider a more complex D-LAA in which three load buses are exploited, with a feedback coming from different generators. Note that, being the optimisation problem not dependant on the on-going attack, the ESS control law is the same as in the previous simulation. In the fourth subplot of Figure 5, the continuous line represents an attack driven by the $(1, 2)$ element of the matrix K^{LG}, the dashed line represents the element $(2, 3)$ while the dotted one represents the element $(4, 3)$. Note that the first two attacks are on buses connected to a generator,

while the last one is on a load bus that has no generator neighbour. The observed behaviour is similar to the previous case, with the system maintaining its stability thanks to the designed CQLF and control.

V. Conclusions and Future Works

The work presented a robust protection scheme against Dynamic Load Altering Attacks to prevent network instability. The results are based on classical Polytopic Linear Differential Inclusion system theory and Lyapunov-Invariance arguments. Simulations validated the approach in a test scenario. Future research will focus on a procedure for the optimal sizing of the invariance ellipsoid used to assure network stable operation, and the ensurance of component-wise constraints on the control effort replacing the bound on its norm assured in the present work. Automatic tuning of the design parameters of the controller will also be explored, to better support the network operator in satisfying its requirements.

VI. Acknowledgments

The authors acknowledge their colleagues of the Network Control Laboratory of the Departmentof Computer, Control, and Management Engineering "Antonio Ruberti" of the University of Rome "La Sapienza" for the fruitful discussions and studies.

References

[1] B. Bohnet, S. Kochanneck, I. Mauser, S. Hubschneider, M. Braun, H. Schmeck, and T. Leibfried, "Hybrid energy storage system control for the provision of ancillary services," in *International ETG Congress 2017*, Nov 2017, pp. 1–6.

[2] B. Kroposki, B. Johnson, Y. Zhang, V. Gevorgian, P. Denholm, B. Hodge, and B. Hannegan, "Achieving a 100electric power systems with extremely high levels of variable renewable energy," *IEEE Power and Energy Magazine*, vol. 15, no. 2, pp. 61–73, March 2017.

[3] Bo Yang, Y. Makarov, J. Desteese, V. Viswanathan, P. Nyeng, B. McManus, and J. Pease, "On the use of energy storage technologies for regulation services in electric power systems with significant penetration of wind energy," in *2008 5th International Conference on the European Electricity Market*, May 2008, pp. 1–6.

[4] A. D. Giorgio, F. Liberati, R. Germanà, M. Presciuttini, L. R. Celsi, and F. Delli Priscoli, "On the control of energy storage systems for electric vehicles fast charging in service areas," in *2016 24th Mediterranean Conference on Control and Automation (MED)*. IEEE, June 2016.

[5] A. K. Srivastava, A. A. Kumar, and N. N. Schulz, "Impact of distributed generations with energy storage devices on the electric grid," *IEEE Systems Journal*, vol. 6, no. 1, pp. 110–117, 2012.

[6] L. Gelazanskas and K. A. Gamage, "Demand side management in smart grid: A review and proposals for future direction," *Sustainable Cities and Society*, vol. 11, pp. 22–30, 2014.

[7] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2011.

[8] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, "Dynamic load altering attacks in smart grid," in *2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb 2015, pp. 1–5.

[9] A. Di Giorgio, A. Giuseppi, F. Liberati, A. Ornatelli, A. Rabezzano, and L. R. Celsi, "On the optimization of energy storage system placement for protecting power transmission grids against dynamic load altering attacks," in *2017 25th Mediterranean Conference on Control and Automation (MED)*, July 2017, pp. 986–992.

[10] F. Adamsky, M. Aubigny, F. Battisti, M. Carli, F. Cimorelli, T. Cruz, A. D. Giorgio, C. Foglietta, A. Galli, A. Giuseppi, F. Liberati, A. Neri, S. Panzieri, F. Pascucci, J. Proenca, P. Pucci, L. Rosa, and R. Soua, "Integrated protection of industrial control systems from cyber-attacks: the atena approach," *International Journal of Critical Infrastructure Protection*, vol. 21, pp. 72 – 82, 2018.

[11] 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, July 2018.

[12] J. C. Geromel and P. Colaneri, "Robust stability of time varying polytopic systems," *Systems & Control Letters*, vol. 55, no. 1, pp. 81–85, 2006.

[13] M. S. Mahmoud, "Switched time-delay systems." Springer, 2010.

[14] H. Lin and P. J. Antsaklis, "Stability and stabilizability of switched linear systems: a survey of recent results," *IEEE Transactions on Automatic control*, vol. 54, no. 2, pp. 308–322, 2009.

[15] H. Horisberger and P. Belanger, "Regulators for linear, time invariant plants with uncertain parameters," *IEEE Transactions on automatic control*, vol. 21, no. 5, pp. 705–708, 1976.

[16] G. Zhai, H. Lin, and P. J. Antsaklis, "Quadratic stabilizability of switched linear systems with polytopic uncertainties," *International Journal of Control*, vol. 76, no. 7, pp. 747–753, 2003. [Online]. Available: https://doi.org/10.1080/0020717031000114968

[17] D. Liberzon, "Switching in systems and control. boston: Birkhäuser," 2003.

[18] D. Liberzon, J. P. Hespanha, and A. S. Morse, "Stability of switched systems: a lie-algebraic condition," *Systems & Control Letters*, vol. 37, no. 3, pp. 117–122, 1999.

[19] H. Lin and P. J. Antsaklis, "Stability and stabilizability of switched linear systems: a survey of recent results," *IEEE Transactions on Automatic control*, vol. 54, no. 2, pp. 308–322, 2009.

[20] B. Polyak and P. Shcherbakov, "Ellipsoidal approximations to attraction domains of linear systems with bounded control," in *2009 American Control Conference*. IEEE, 2009, pp. 5363–5367.

[21] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. McGraw-hill New York, 1994, vol. 7.

[22] F. Pasqualetti, A. Bicchi, and F. Bullo, "A graph-theoretical characterization of power network vulnerabilities," in *Proceedings of the 2011 American Control Conference*, June 2011, pp. 3918–3923.

[23] P. W. Sauer and M. A. Pai, *Power system dynamics and stability*. Prentice hall Upper Saddle River, NJ, 1998, vol. 101.