Defense against DoS and load altering attacks via model-free control: A proposal for a new cybersecurity setting

Michel Fliess, Cédric Join, Dominique Sauter

Defense against DoS and load altering attacks via model-free control: A proposal for a new cybersecurity setting

Michel Fliess[1,3], Cédric Join[2,3] and Dominique Sauter [2]

***Abstract*— Defense against cyberattacks is an emerging topic related to fault-tolerant control. In order to avoid difficult mathematical modeling, model-free control (MFC) is suggested as an alternative to classical control. For illustration purpose a Load Frequency Control of multi-areas power network is considered. In the simulations, load altering attacks and Denial of Service (DoS) in the communication network are applied to the system. Our aim is to compare the impact of cyberattacks on control loops closed via respectively a classical controller in such situations and a model-free one. Computer experiments show impressive results with MFC.**

***Index Terms*— Cyberattacks, load altering attacks, Denial of Service, fault-tolerant control, actuator's fault accommodation, packet loss, power grid, load frequency control, model-free control.**

I. Introduction

The design of secure and safe *Networked Control System* (*NCS*) is of high importance in the control of large-scale critical infrastructures or industrial plants such as power grids, transportation systems, communication networks, oil and gas pipelines, water distribution or waste-water treatment systems and irrigation networks [1]. Using "open" public and also wireless networks for the communication within NCS can generate severe security problems since an unauthorized access ("cyberattack") is possible in the control system. The security of control systems against malicious attacks has received a great deal of attention over the past few years, in particular after the Stuxnet attack against Iran nuclear installations in 2010 [2]. Specific analysis tools as well as monitoring mechanisms have been developed to enforce system security and reliability [3], [4]. Information security approach may provide some protection methods that help in improving the security of control systems, but these methods appear to be not sufficient for the defense of the systems against malicious attacks able to bypass information security layers, as in the case of Stuxnet incident in 2010. As pointed out in [5] the security of *Cyber-Physical Systems* (*CPS*) integrating computation, communication and physical capabilities must be improved from both information technology and control theory. The *cyber-physical attacks* (*CPA*), on both the physical layer and the cyber layer, are modeled as additive signals of short duration on both system equations. Attackers can break into the communication channels, enabling them to modify the command signals, control signals or sensor measurements for disrupting the systems. CPA in CPS, summarized in [5], [6], [7], may be divided into several categories:

- *Denial of Service* (*DoS*) attacks in [8], [9]: adversaries aim at disrupting temporarily or indefinitely the exchange of data among entities in the network.
- *Integrity* or *Man in The Middle* (*MITM*) attacks in [10], [11], [12], [13], [14]: adversaries inject false data on control signals or on information transmitted by sensors to the plant via communication channels, and finally physical attacks on sensors and actuators close to faults.
- *Replay attack* in [15] can be viewed as a deception attack on control signals coordinated with the generation of artificial delays on measurements.

Among such a huge number possibilities (see also [16], [17], [18], [19]), we concentrate here on Denial of Service and *load altering attacks* which correspond to a large body of concrete situations. The defense against those strikes is connected to a classic topic in control engineering, namely *fault-tolerant control* (see, *e.g.*, [20], [21]), *i.e.*, a set of techniques for mitigating the effects of the unavoidable faults which occur in any control system.

Model-free control, or *MFC*, in the sense of [22], [23] is chosen for the following reasons:

- It has been already successfully applied many times (see, *e.g.*, [24] for an automated vehicle) including in fault-accommodation [25], [26].
- Most of the existing defense approaches rely on a mathematical modeling (see, *e.g.*, [27], [28], [29], [30], [31] for power systems) which too often is most difficult to derive. A model-free setting might therefore be fruitful (see, *e.g.*, [32], [33], [34]).
- Load altering attacks ought to be related to actuator's faults. It has been proven [22], [25] that model-free control is quite efficient in actuator's fault accommodation.
- Some DoS attacks might look as *packet losses* (see, *e.g.*, [35]). It has been shown [36] via numerical and concrete experiments that model-free control exhibits excellent performances in spite of severe losses.

Our proposal is illustrated by several computer experiments. They are based on [37], [38] where

- the application of network technology in the power grid makes the *load frequency control* (*LFC*) system more vulnerable to various kinds of attacks (see, *e.g.*, [39] for a general presentation);

[1]LIX (CNRS, UMR 7161), École polytechnique, 91128 Palaiseau, France
Michel.Fliess@polytechnique.edu
[2]CRAN (CNRS, UMR 7039)), Université de Lorraine, BP 239, 54506 Vandœuvre-lès-Nancy, France
{cedric.join, dominique.sauter}@univ-lorraine.fr
[3]AL.I.E.N., 7 rue Maurice Barrès, 54330 Vézelise, France
{michel.fliess, cedric.join}@alien-sas.com

- DoS and load alteration attacks fit very well.

Our paper is organized as follows. Section II reviews MFC which is certainly unknown to most of the experts in cybersecurity. In particular Section II-E explains how to react against load altering attacks. Computer experiments are displayed in Section III with many Figures and 2 Tables, which show the efficiency of our approach. Some concluding remarks may be found in Section IV.

II. What is model-free control?

A. Ultra-local model

The unknown global description of the plant is replaced by the following first-order *ultra-local model*:

$$\dot{y} = F + \alpha u \tag{1}$$

where:

1) The control and output variables are respectively u and y.
2) $\alpha \in \mathbb{R}$ is chosen by the practitioner such that the three terms in Equation (1) have the same magnitude.

The following comments are useful:

- F is *data driven*: it is given by the past values of u and y.
- F includes not only the unknown structure of the system but also any disturbance.

B. Intelligent controllers

Close the loop with the *intelligent proportional controller*, or *iP*,

$$u = -\frac{F_{\text{est}} - \dot{y}^* + K_P e}{\alpha} \tag{2}$$

where

- y^* is the reference trajectory,
- $e = y - y^\star$ is the tracking error,
- F_{est} is an estimated value of F
- $K_P \in \mathbb{R}$ is a gain.

Equations (1) and (2) yield

$$\dot{e} + K_P e = F - F_{\text{est}}$$

If the estimate F_{est} is "good": $F - F_{\text{est}}$ is "small", *i.e.*, $F - F_{\text{est}} \simeq 0$, then $\lim_{t\to+\infty} e(t) \simeq 0$ if $K_P > 0$. It implies that the tuning of K_P is straightforward. This is a major difference with the tuning of "classic" PIDs (see, *e.g.*, [40]).

C. Estimation of F

A real-time estimate of F is given by (see [22] for more details)

$$F_{\text{est}}(t) = -\frac{6}{\tau^3}\int_{t-\tau}^{t} \left[(\tau - 2\sigma)y(\sigma) + \alpha\sigma(\tau - \sigma)u(\sigma)\right] d\sigma \tag{3}$$

where $\tau > 0$ is "small." This integral, which is a low pass filter, may of course be replaced in practice by a classic digital filter.

D. MIMO systems

Consider a multi-input multi-output (MIMO) system with m control variables u_i and m output variables y_i, $i = 1, \ldots, m$, $m \geq 2$. It has been observed in [25] and confirmed by all encountered concrete case-studies (see, *e.g.*, [41]), that such a system may usually be regulated via m monovariable ultra-local models:

$$\dot{y}_i = F_i + \alpha_i u_i$$

where F_i may also depend on u_j, y_j, and their derivatives, $j \neq i$.

E. Actuator's fault accommodation

We assume that cyberattacks can be represented as additive signals applied to the controller output. In Equation (1) write the input variable

$$u = u_{\text{attack}} + v$$

where u_{attack} (resp. v) is an unwanted (resp. the desired) quantity. It yields

$$\dot{y} = \mathfrak{F} + \alpha v$$

where

$$\mathfrak{F} = F + \alpha u_{\text{attack}}$$

It is straightforward to adapt the iP (2)

$$v = -\frac{\mathfrak{F}_{\text{est}} - \dot{y}^* + K_P e}{\alpha}$$

and the estimate $\mathfrak{F}_{\text{est}}$ of $\mathfrak{F}$ in Formula (3)

$$\mathfrak{F}_{\text{est}}(t) = -\frac{6}{\tau^3}\int_{t-\tau}^{t} \left[(\tau - 2\sigma)y(\sigma) + \alpha\sigma(\tau - \sigma)v(\sigma)\right] d\sigma$$

III. Application to power network

In power systems, LFC used for frequency stabilization [42], [43] is one of the most essential operational functions. Considering interconnected generation/distribution systems the main objective of LFC is to ensure the balance between load and generation in each control area [44], [45], [46]. However, the LFC system in modern power systems tends to use open communication networks to transmit control/measurement signals, thus making the LFC system more vulnerable to cyberattacks such as denial of service (DOS) attacks.

Defense against cyberattacks is an emerging topic for power transmission and distribution systems [47], [48]. While many works focus on detection [49], [50] and isolation of the attack signal, few of them actually consider the design of a complete defense mechanism, which is essential for the robustness of the control system under attack.

To date, many researchers have applied a significant effort in favor of the LFC system regarding the defense against DoS attacks. Considering DoS attacks as network-induced sent disturbances, some robust LFC systems for interconnected power systems have been developed as for example in [27], [28], [29], [30]. Nevertheless, most of these approaches rely on the knowledge of a model of the LFC system. More recently another *model-free* approach, inspired by *fault tolerant control* (*FTC*) [51], has been proposed [52], [53].

A. Power grid

A large power system consists of a number of interconnected control areas, which are connected by tie lines. The LFC is used to maintain the system frequency and power exchange between the tie lines at a predefined value (see, *e.g.*, [39]). As illustrated in Figure 1, the typical components of an LFC system installation are the controller, turbine, generator and load. The input to the controller is the *Area Control Error*, or *ACE*. The ACE is defined for each zone as a linear combination of the total power exchanged and the frequency deviations from the respective programmed and nominal values. The LFC system relies on the communication between the sensors and the *Energy Management System*, or *EMS*, and is therefore exposed to high risks of cyber-intrusion. In the device displayed in Figure 1 load variations are mitigated via phase shift minimization by two generators (see [37], [38] for more details). Note moreover that power grids were already investigated via model-free control [54], [55].

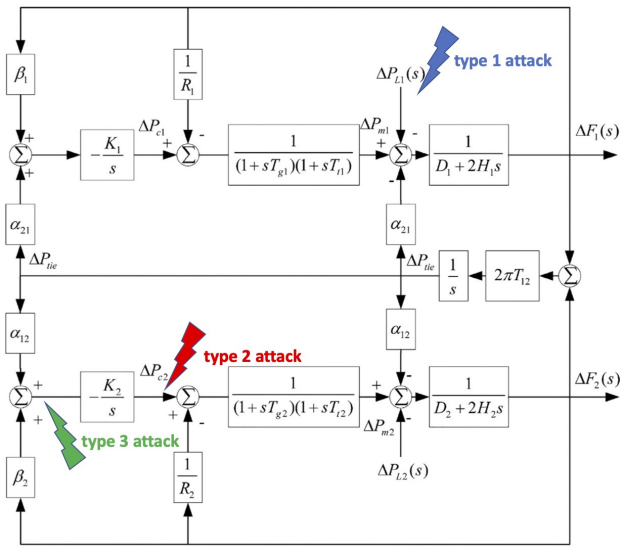


Fig. 1: Block diagram of a power system

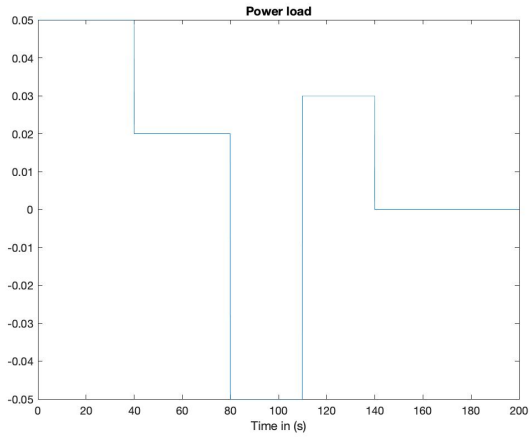


Fig. 2: Nominal load variations

Three types of attacks are considered:

1) **Type 1 attack (blue)**: very important additive load variation of short time (load altering attack).
2) **Type 2 attack (red)**: blocking the control to generator 2 (DoS attack).
3) **Type 3 attack (green)**: blocking the measures of generator 2 (DoS attack).

The pure integrators $\frac{K_1}{s}$, $\frac{K_2}{s}$ in Figure 1 are replaced by two model-free controllers defined by Equations (1)-(2) in order to insure a better defense. See [56], which is devoted to traffic regulation on motorways, for a similar result.

B. Various scenarios

In all our computer simulations, $K_1 = K_2 = 1$, and $\alpha = 10$, $K_P = 0.3$ in Formula (2). Pure integrators are compared to model-free control. The load variations, which are depicted in Figure 2, are identical.

1) No attack: Figures 3 and 4.
2) Type 1 load altering attack: Figures 5 and 6.
3) Type 2 DoS attack with 90% *losses:* Figures 7 and 8.
4) Type 3 DoS attack with 95% *losses:* Figures 9 and 10.

For each scenario, constant reference trajectory and load frequency are presented on subfigure (a) (resp. (c)) for line/area 1 (resp. 2). Subfigure (b) (Resp. (d)) draws the power control for line/area 1 (resp. 2).

Without any attack, two control strategies seem to have similar behavior but, as shown in Table I, the trajectory tracking error decreases significantly with our proposition.
With type 1 attack, as illustrated in Figures 5 and 6 and in Table I, better results, especially for area 2, are obtained with MFC.
The superiority of the model-free setting becomes crushing with in the case of DoS attacks. This is also highlighted by Table II: It summarizes 100 simulations where the selection of packet loss is random and in the same proportion.

IV. Conclusion

From a theoretical standpoint let us emphasize the two following remarks

1) The defense again load altering attacks is mathematically well justified in Section II-E.
2) The dazzling efficiency against DoS attacks is based only on computer experiments, *i.e.*, on *experimental mathematics* (see, *e.g.*, [57]). A formal proof is lacking today.

Our proposal for cybersecurity, in order to be more convincing, needs of course further investigations, for instance on control saturation.

References

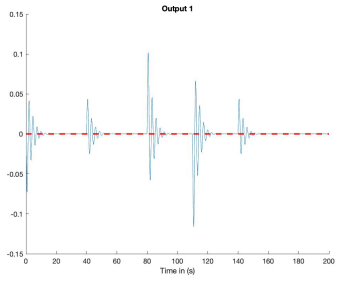
[1] K. Stouffer, J. Falco, K. Scarfone, Guide to industrial control systems (ics) security. NIST Spec. Public., vol. 800-82, 2007.
[2] N. Falliere, Exploring stuxnet's plc infection process. http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process, 2010.
[3] I.N. Fovino, A. Coletta, M. Masera,Taxonomy of security solutions for scada sector. JRC-Joint Research Centre Europ. Commiss., 2010.
[4] R.L. Krutz (2005). Securing SCADA systems. Wiley, 2005

TABLE I: Sum of tracking errors for 2 lines

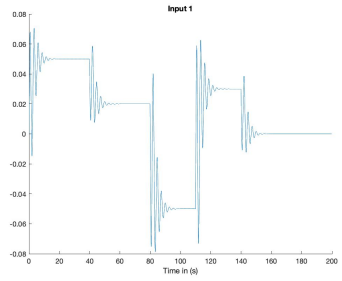
Control types/scenarios	$\Sigma_t\|e_1\|$	$\Sigma_t e_1^2$	$\Sigma_t\|e_2\|$	$\Sigma_t e_2^2$
Integrator/scenario 1	9.1106	0.3763	2.8981	0.0283
MFC/scenario 1	6.7965	0.2832	1.7452	0.0118
Integrator/scenario 2	29.4256	4.6806	9.3662	0.3597
MFC/scenario 2	21.8710	3.4752	5.5665	0.1418

TABLE II: Sum of tracking errors for 2 lines: Averaging 100 simulations

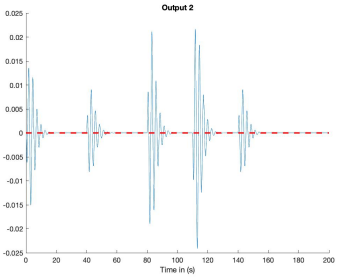
Control types/scenarios	$\Sigma_t\|e_1\|$	$\Sigma_t e_1^2$	$\Sigma_t\|e_2\|$	$\Sigma_t e_2^2$
Integrator/scenario 3	212.0977	$1.8926.10^4$	$1.3241.10^3$	$5.8470.10^5$
MFC/scenario 3	7.3609	0.2884	2.5912	0.0232
Integrator/scenario 4	$6.0832.10^9$	$1.2731.10^{19}$	$2.4134.10^{10}$	$1.7941.10^{20}$
MFC/scenario 4	9.6472	0.5017	11.1365	2.4834



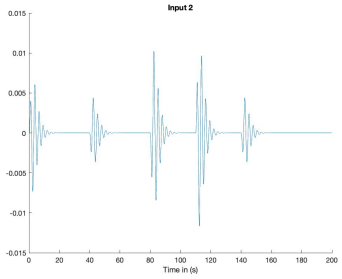
(a) Output (–) and reference trajectory (- -) line 1



(b) Control line 1



(c) Output (–) and reference trajectory (- -) line 2



(d) Control line 2

Fig. 3: Integrator: No attack

[5] A. Cardenas, S. Amin and S. Sastry, Secure control: Towards survivable cyber-physical systems. 1st Int. Worksh. Cyber-Phys. Syst., Beijing, 2008.

[6] F. Pasqualetti, Secure Control Systems: A Control-Theoretic Approach to Cyber-Physical Security. PhD, University of California, 2012.

[7] F. Pasqualetti, F Dorfler, F. Bullo, Attack detection and identification in cyber-physical systems. IEEE Trans. Automat. Contr., vol. 58, 2715-2729, 2013.

[8] S. Amin, A. Cardenas, S. Sastry, Safe and secure networked control systems under denial-of-service attacks. R. Majumdar & P. Tabuada (Eds): Hybrid Systems: Computation and Control, Lect. Notes Comput. Sci. 5469, 31-45, 2009.

[9] Y.L. Huang, A.A. Cárdenas, S. Amin, Z.S. Lin, H.Y. Tsai, S. Sastry. Understanding the physical and economic consequences of attacks on control systems. Int. J. Critic. Infrastruct. Protect., vol. 2, 73-83, 2009.

[10] Y. Liu, M.K. Reiter, P. Ning, False data injection attacks against state estimation in electric power grids, ACM Conf. Comput. Communicat. Secur., Chicago, 2009.

[11] A. Teixeira, H. Sandberg, K.H. Johansson, Networked control system under cyber attacks with applications to power networks, Amer. Contr. Conf., Baltimore, 2010.

[12] R.S. Smith, A decoupled feedback structure for covertly appropriating networked control systems. World IFAC Congr., Zurich, 2011.

[13] A. Teixeira, D. Perez, H. Sandberg, K.H. Johansson, Attack models and scenarios for networked control systems. 1st Int. Conf. High Confid. Network. Syst., Beijing, 2012.

[14] F. Pasqualetti, F. Dorfler, F. Bullo, Cyber-physical security via geometric control: Distributed monitoring and malicious attacks. 51st IEEE Conf. Decis. Contr., Maui, 2012.

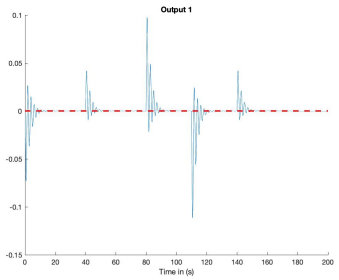
[15] Y. Mo, B. Sinopoli, Secure control against replay attacks, Allerton Conf. Commun. Contr. Comput., Monticello, 2010.

[16] H.S. Sánchez, D. Rotondo, J. Quevedo, Bibliographical review on cyber attacks from a control oriented perspective. Ann. Rev. Contr., vol. 48, 103-128, 2019.

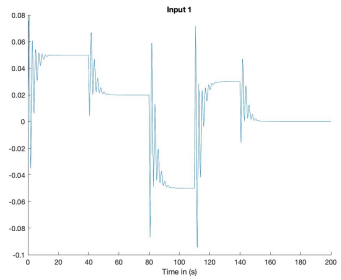
[17] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin, Cybersecurity for industrial control systems: A survey. Comput. Secur., vol. 89, 101677, 2020.

[18] M.M. Hossain, C. Peng, Cyber-physical security for on-going smart grid initiatives: a survey. IET Cyber-Phys. Syst. Theory Appl., vol. 5, 233-244, 2020.

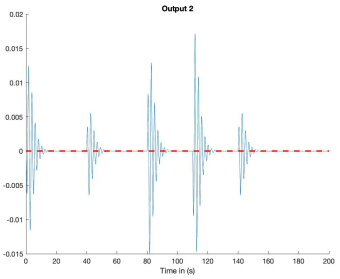
[19] L. Zhao, W. Li, Co-design of dual security control and communication for nonlinear CPS under DoS attack. IEEE Access, vol. 8, 19271-



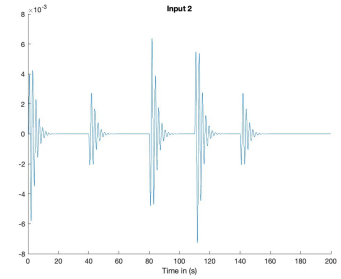
(a) Output (–) and reference trajectory (- -) line 1



(b) Control line 1

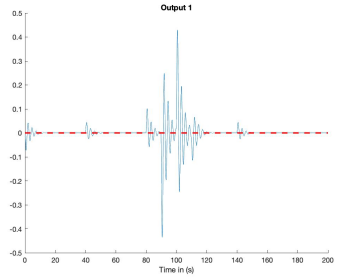


(c) Output (–) and reference trajectory (- -) line 2

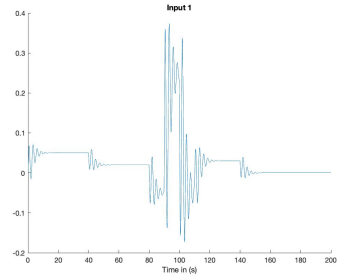


(d) Control line 2

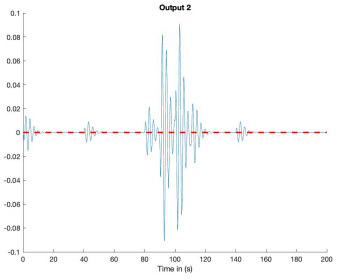
Fig. 4: MFC: No attack



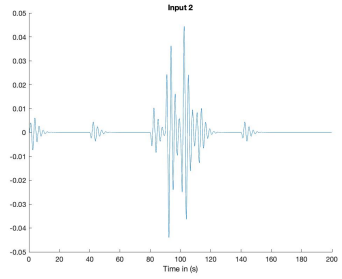
(a) Output (–) and reference trajectory (- -) line 1



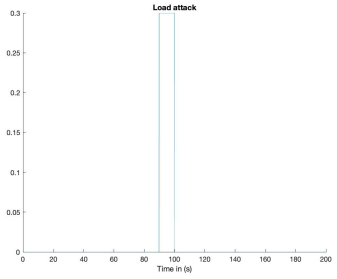
(b) Control line 1



(c) Output (–) and reference trajectory (- -) line 2



(d) Control line 2



(e) Abrupt change of power load

Fig. 5: Integrator: Load altering attack

19285, 2020.

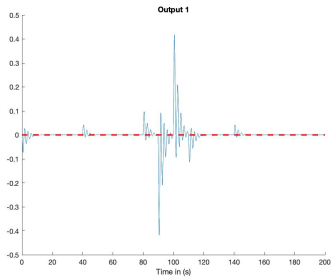
[20] H. Noura, D. Theilliol, J.-C. Ponsart, D. Chamseddine, Fault-tolerant Control Systems: Design and Practical Applications. Springer, 2009.

[21] M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki, Diagnosis and Fault-Tolerant Control (3rd ed.). Springer, 2016.

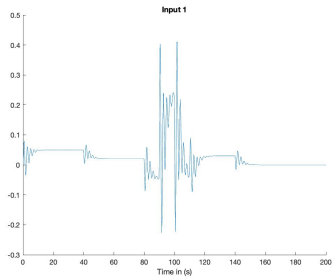
[22] M. Fliess, C. Join, Model-free control., Int. J. Contr., vol. 86, 2228-2252, 2013.

[23] M. Fliess, C. Join, An alternative to proportional-integral and proportional-integral-derivative regulators: Intelligent proportional-derivative regulators. Int. J. Robust Nonlinear Contr., 2021. https://doi.org/10.1002/rnc.5657

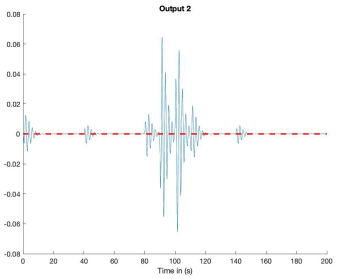
[24] Z. Wang, J. Wang, Ultra-local model predictive control: A model-free



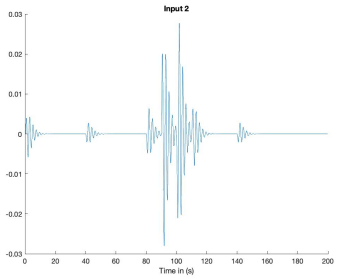
(a) Output (–) and reference trajectory (- -) line 1



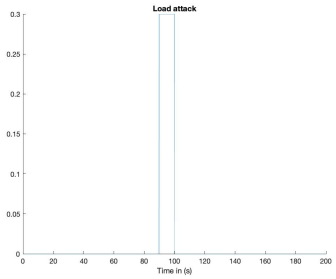
(b) Control line 1



(c) Output (–) and reference trajectory (- -) line 2

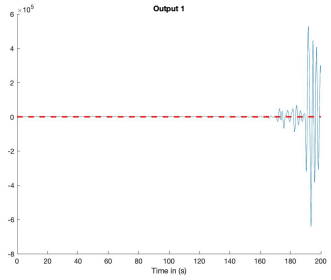


(d) Control line 2

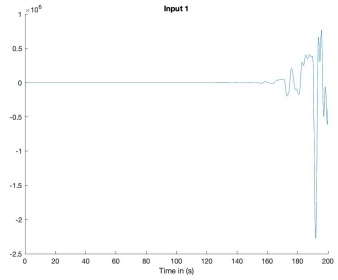


(e) Abrupt change of power load

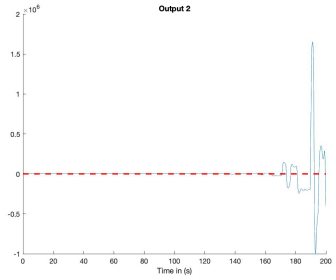
Fig. 6: MFC: Load altering attack



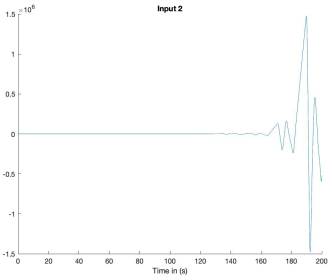
(a) Output (–) and reference trajectory (- -) line 1



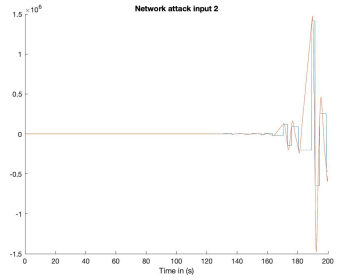
(b) Control line 1



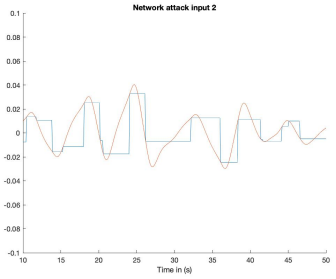
(c) Output (–) and reference trajectory (- -) line 2



(d) Control line 2



(e) Attack-free control (red) and control after attack (blue)



(f) Zoom on (c)

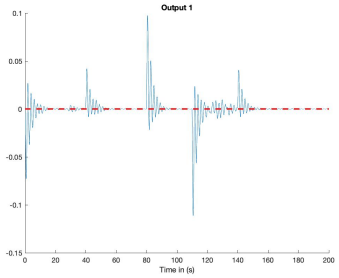
Fig. 7: Integrator: Type 2 DoS attack

approach and its application on automated vehicle trajectory tracking. Contr. Engin. Pract., vol. 101, 104482, 2020.

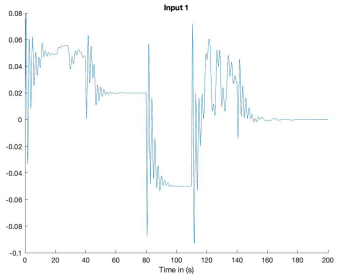
[25] F. Lafont, J.-F. Balmat, N. Pessel, M. Fliess, A model-free control strategy for an experimental greenhouse with an application to fault accommodation. Comput. Electron. Agricult., vol. 110, 139-149, 2015.

[26] B. Park, M.M. Olama, A model-free voltage control approach to mitigate motor stalling and FIDVR for smart grids. IEEE Trans. Smart Grid, vol. 12, 67-78, 2021.

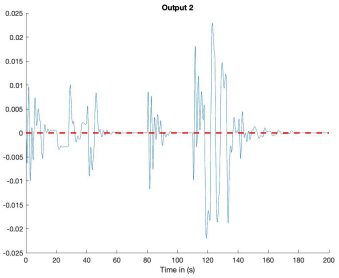
[27] H.H. Alhelou, M.E. Hamedani-Golshan, N.D. Hatziargyriou, A decentralized functional observer based optimal LFC considering unknown inputs, uncertainties, and cyber-attacks. IEEE Trans. Power Syst., vol. 34, 4408-4417, 2019.



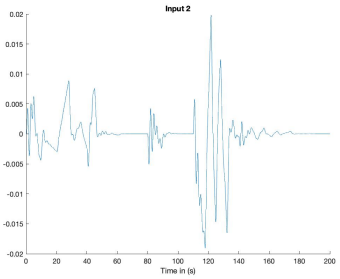
(a) Output (–) and reference trajectory (- -) line 1



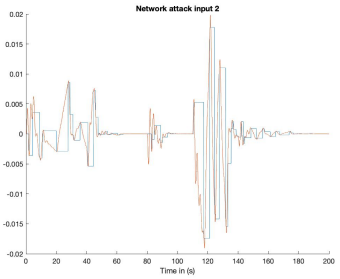
(b) Control line 1



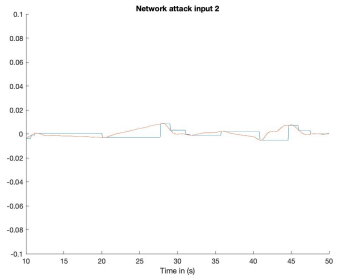
(c) Output (–) and reference trajectory (- -) line 2



(d) Control line 2

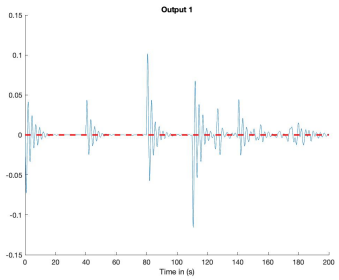


(e) Attack-free control (red) and control after attack (blue)

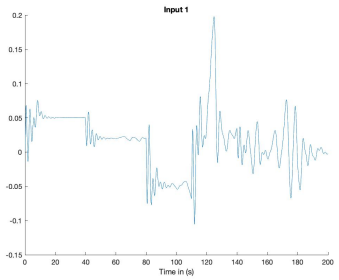


(f) Zoom on (c)

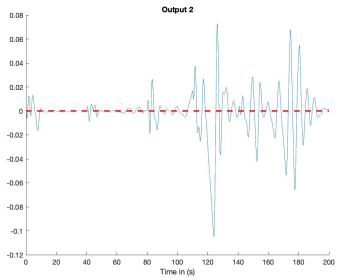
Fig. 8: MFC: Type 2 DoS attack



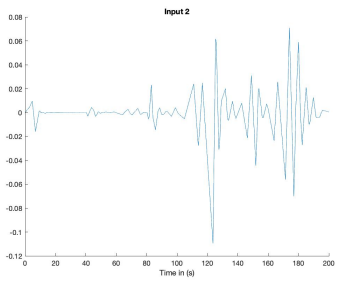
(a) Output (–) and reference trajectory (- -) line 1



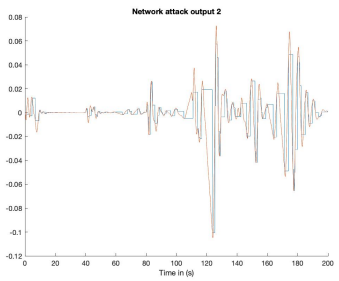
(b) Control line 1



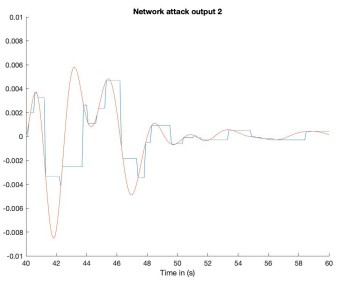
(c) Output (–) and reference trajectory (- -) line 2



(d) Control line 2



(e) Attack-free measured output (red) and measured output after attack (blue)



(f) Zoom on (c)

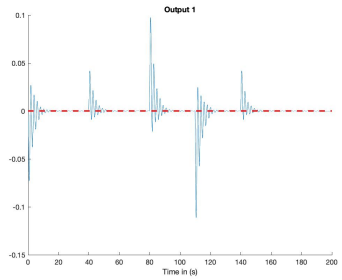
Fig. 9: Integrator: Type 3 DoS attack

[28] X. Liu, Y. Zhang, Y., K.Y. Lee, Robust distributed MPC for load frequencycontrol of uncertain power systems. Contr. Engin. Pract., vol. 56, 23-47, 2016.

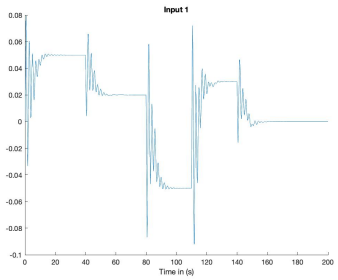
[29] S. Saxena, Y.V. Hote, Stabilization of perturbed system via IMC: An application to load frequency control. Contr. Engin. Pract., vol. 64, 61-73, 2017.

[30] J. Liu, Y. Gu, L. Zha, J. Cao, Event-triggered load frequency control formultiarea power systems under hybrid cyber attacks. IEEE Trans. Syst. Man Cybernet.: Syst., vol. 49, 1665-1678, 2019..

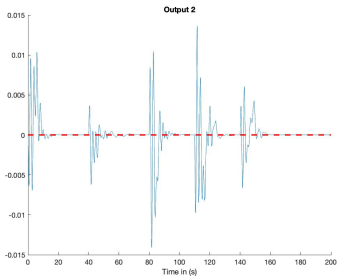
[31] M.M. Hossain, C. Peng, Observer-based event triggering H_∞ LFC for multi-area power systems under DoS attacks. Informat. Sci., vol. 543, 437-453, 2021.



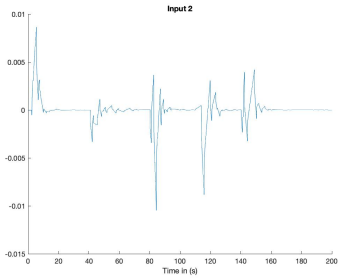
(a) Output (–) and reference trajectory (- -) line 1



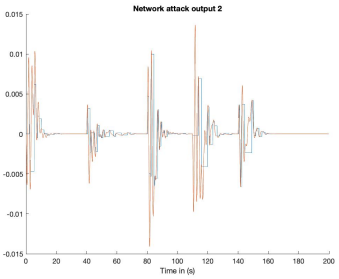
(b) Control line 1



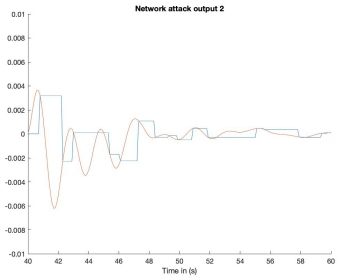
(c) Output (–) and reference trajectory (- -) line 2



(d) Control line 2



(e) Attack-free measured output (red) and measured output after attack (blue)



(f) Zoom on (c)

Fig. 10: MFC: Type 3 DoS attack

[32] M.S. Kemal, W. Aoudi, R.L. Olsen, M. Almgren, H.-P. Schwefel, Model-free detection of cyberattacks on voltage control in distribution grids. 15th Europ. Depend. Comput. Conf., Naples, 2015.

[33] C. Chen, M. Cui, X. Fang, B. Ren, Y. Chen, Load altering attack-tolerant defense strategy for load frequency control system. Appli. Energ., vol. 280, 116015, 2020.

[34] X. Qiu, Y. Wang, X. Xie, H. Zhang, Resilient model-free adaptive control for cyber-physical systems against jamming attack. Neurocomput., vol. 413, 422-430, 2020.

[35] H. Lin, H. Su, P. Shi, Z. Shu, Z.-G. Wu, Estimation and Control for Networked Systems with Packet Losses without Acknowledgement. Springer, 2017.

[36] C. Join, M. Fliess, F. Chaxel, Model-free control as a service in the Industrial Internet of Things: Packet loss and latency issues via preliminary experiments. 28th Medit. Conf. Contr. Automat., Saint-Raphaël, 2020. https://hal.archives-ouvertes.fr/hal-02546750/en/

[37] T.C. Yanga, Z.T. Ding, H. Yu, Decentralised power system load frequency control beyond the limit of diagonal dominance, Electric. Power Energy Syst., vol. 24, 173-184, 2002.

[38] Y. Lia, P. Zhang, L. Ma, Denial of service attack and defense method on load frequency control system, J. Franklin Instit., vol. 356, 8625-8645, 2019.

[39] H. Bevrani, Robust Power System Frequency Control (2nd ed.). Springer, 2014.

[40] K.J. Åström, R.M. Murray, Feedback Systems: An Introduction for Scientists and Engineers. Princeton University Press, 2008.

[41] Y. Wang, H. Li, R. Liu, L. Yang, X. Wang, X., Modulated model- free predictive control with minimum switching losses for PMSM drive system, IEEE Access, vol. 8, 20942-20953, 2020.

[42] P. Kundur, Power system stability and control. McGraw Hill, 1994.

[43] J. Sharma, Y. V. Hote, R. Prasad, PID controller design for interval load frequency control system with communication time delay. Contr. Engin. Pract., vol. 9, 154-168, 2019.

[44] L. Jiang, W. Yao, Q. H. Wu, J. Y.,Wen, S. J. Cheng, Delay-dependent stability for load frequency control with constant and time-varying delays. IEEE Trans. Power Syst., vol. 27, 932-941, 2012.

[45] A. Khodabakhshian, M. Edrisi, A new robust PID load frequency controller. Contr. Engin. Pract., vol. 16, 1069-1080, 2008.

[46] H. H. Alhelou, M. E. Hamedani-Golshan, R. Zamani, E. Heydarian-Forushani, P. Siano, Challenges and opportunities of load frequency control in conventional, modern and future smart power systems: A comprehensive review. Energies, vol. 11, 2497, 2018.

[47] S. Mishra, K. Anderson, B. Miller, K. Boyer, A. Warren, Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. Appl. Energy, vol. 264, 114726, 2020.

[48] M. Z. Gunduz, R. Das, Cyber-security on smart grid: Threats and potential solutions. Comput. Netw., vol. 169, 107094, 2020

[49] D. Zhang, Q.G. Wang, G.F. YangShi, A.V. Vasilakos, A survey on attack detection, estimation and control of industrial cyber-physical systems. ISA Trans., 2021

[50] D.B. Rawat, C. Bajracharya, Detection of false data injection attacks in smart grid communication systems. IEEE Signal Process Lett, vol. 22, 1652-1654, 2015.

[51] H. Noura, D. Sauter, F. Hamelin, D. Theilliol, Fault-tolerant control in dynamic systems: Application to a winding machine. IEEE Contr. Syst. Magaz., vol. 20, 33-49, 2000.

[52] C. Chen , M. Cui , X. Fang , B. Ren, Y. Chen, Load altering attack-tolerant defense strategy for load frequency control system. Appl. Energy, vol. 280, 2020.

[53] X. Qiu, Y. Wang, X. Xie, H. Zhang Resilient model-free adaptive control for cyber-physical systems against jamming attack. Neurocomput., vol. 413, 422-430, 2020.

[54] A. Barkat, B. Marinescu, C. Join, M. Fliess, Model-free control for VSC-based HVDC systems. IEEE PES Innovat. Smart Grid Techno. Conf. Euro., Sarajevo, 2018. https://hal.archives-ouvertes.fr/hal-01820886/en/

[55] M. Ferrari, B. Park, M.M. Olama, Design and evaluation of a model-free frequency control strategy in islanded microgrids with power-hardware-in-the-loop testing. IEEE Pow. Ener. Soc. Innov. Smart Grid Tech. Conf., Washington, 2021.

[56] H. Abouaïssa, M. Fliess, C. Join, On ramp metering: towards a better understanding of ALINEA via model-free control. Int. J. Contr., vol. 90, 1018-1026, 2017.

[57] V.I. Arnold, Experimental Mathematics (translated from the Russian), Math. Sci. Res. Instit., 2015.