Distributed Attack Monitoring Scheme for Islanded DC Microgrids

A. J. Gallo, **M. S. Turan**[1], P. Nahata, F. Boem, T. Parisini, G. Ferrari-Trecate

1. EPFL, mustafa.turan@epfl.ch

Imperial College London

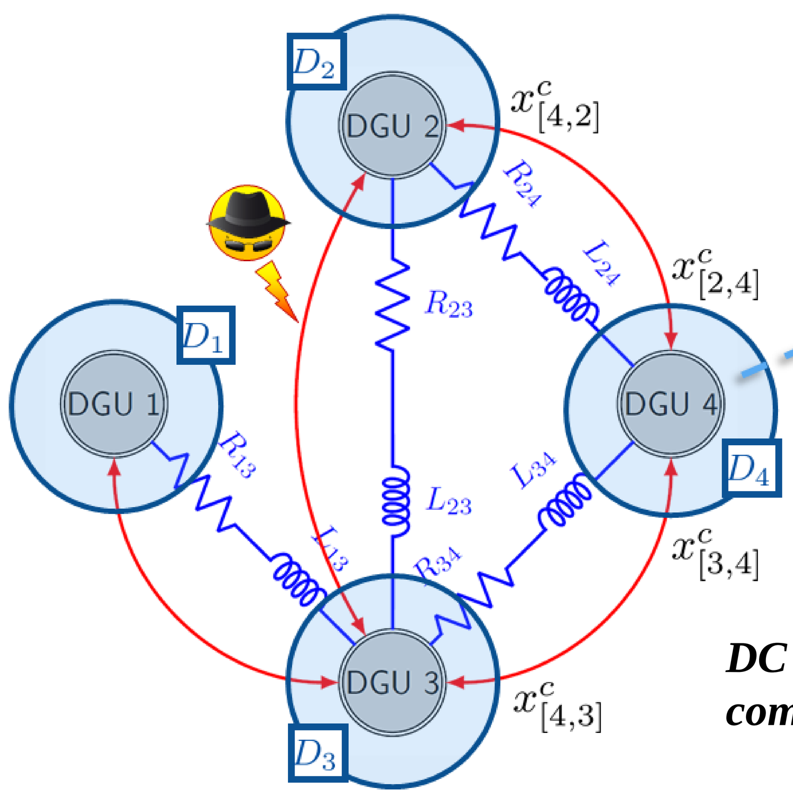
EPFL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

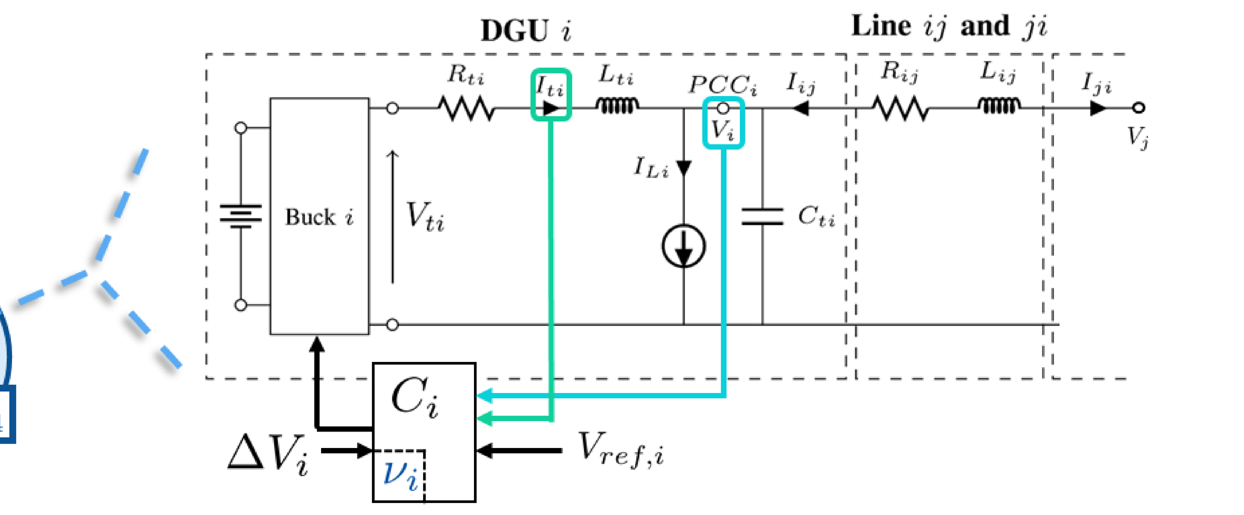
UCL

KIOS

Objectives

- Design distributed monitoring scheme for islanded DC microgrids;
- Detect attacks on communication network connecting Distributed Generation Units (DGUs);
- Ensure monitoring scheme is scalable with size of microgrid.





DC microgrid: physically interconnected DGUs with communication network and monitoring units

DC Microgrid Structure and Control

Network of ***physically interconnected*** Distributed Generation Units (DGUs). DGU state $x_{[i]} = [V_i\,,\, I_{ti}\,,\, \nu_i]^\top$ with physically coupled dynamics:

$$
DGU_i : \begin{cases}
\dot{V}_i = \frac{1}{C_{ti}} I_{ti} + \underbrace{\sum_{j\in\mathcal{N}_i} \frac{1}{R_{ij}C_{ti}}(V_j - V_i)}_{\text{physical coupling}} - \frac{1}{C_{ti}} I_{Li} + \underbrace{noise}_{\text{bounded}} \\
\dot{I}_{ti} = \frac{1}{L_{ti}} V_{ti} - \frac{R_{ti}}{L_{ti}} I_{ti} - \frac{1}{L_{ti}} V_i + \underbrace{noise}_{\text{bounded}} \\
\dot{\nu}_i = V_{ref} + \Delta V_i - V_i + \underbrace{noise}_{\text{bounded}}
\end{cases}
$$

All states measurable: $x^m_{[i]} = x_{[i]} + \overbrace{noise}^{\text{bounded}}$

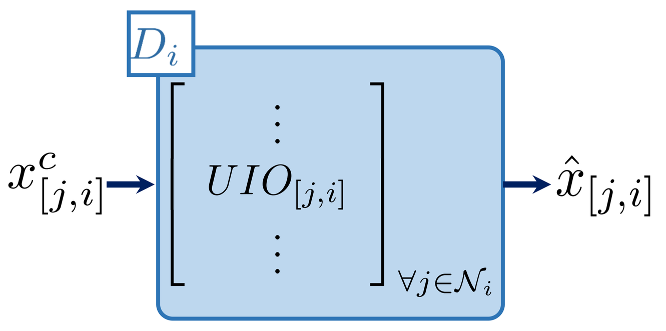
Control architecture

- Decentralized primary control $V_{ti} = K_i x^m_{[i]}$
- Distributed consensus-based secondary control $\Delta \dot{V}_i \propto \sum_{j\in\mathcal{N}_i} \underbrace{(I^m_{ti} - I^c_{tj})}_{\text{cyber coupling}}$
  - ➢ Requires **communication network**
  - ➢ Introduces opportunity for ***attack*** over communication network
    - ➢ Communicated measurement:

$$x^c_{[j,i]} = x^m_{[j]} + \underbrace{\phi_{j,i}(t)}_{\text{attack}}$$

Microgrid Security

UIO-based monitors



Bank of UIOs estimating state of neighboring DGUs

Distributed Unknown Input Observer-based attack **detectors** D_i. Each DGU i monitors the state of each of its neighbors. UIO structure grants independence from interconnection and input variables unknown to DGU i without them being transmitted.

UIO dynamics:
$$
\begin{cases}
\dot{z}_{[j,i]}(t) = F_j z_{[j,i]}(t) + T_j B \bar{u}_{[j]}(t) + \widehat{K}_j x^c_{[j,i]}(t) \\
\hat{x}_{[j,i]}(t) = z_{[j,i]}(t) + H_j x^c_{[j,i]}(t)
\end{cases}
$$

where:
$$(H_j C_j - I) E_j = 0 \quad \rightarrow \text{Decouple Unknown Inputs}$$
$$T_j = I - H_j C_j$$
$$F_j = T_j A_{Kj} - \widetilde{K}_j C_j \quad \rightarrow \text{Provide Stability}$$
$$\bar{K}_j = F_j H_j$$
$$\widehat{K}_j = \widetilde{K}_j + \bar{K}_j$$

$$\underbrace{r_{[j,i]}}_{x^c_{[j,i]} - \hat{x}_{[j,i]}} \not\propto \left[\underbrace{I_{Lj},\, V_{ref},\, \Delta V_j,\, x^\top_{[k\in\mathcal{N}_j]}}_{\text{unknown to DGU } i}\right]^\top$$

Threshold based detection

Residual error bounded by a time-varying threshold:

- Bound computed from bounds on noise and UIO error stability
- Upper bounds on noise ⟶ absence of false alarms guaranteed by design

If $\underbrace{\left|r_{[j,i]}\right|}_{x^c_{[j,i]} - \hat{x}_{[j,i]}} > \bar{r}_{[j,i]}$ ➡ Attack present

Detection logic

Information required

To implement this detection scheme, DGU i requires from each of its neighbors:

- at design time, partial dynamics and bounds on noise
- at running time, communicated variable $x^c_{[j,i]}$

Detection Properties

Detectability analysis

Given initial time of attack T_a, an attack is ***guaranteed* to be detected** by the monitoring scheme if there is a time t at which the following holds for at least one component:

$$\left| e^{F_j(t-T_a)} H_j \phi_{j,i}(T_a) + T_j \phi_{j,i}(t) - \int_{T_a}^{t} e^{F_j(t-\tau)} \left[\widehat{K}_j \phi_{j,i}(\tau)\right] d\tau \right| > 2\bar{r}_{[j,i]}(t)$$

Stealthy Attacks

➢ An attack is said to be ***stealthy*** if it is not detectable.

It is sufficient for an attack to satisfy the following for it to be stealthy to the UIO-based detection strategy

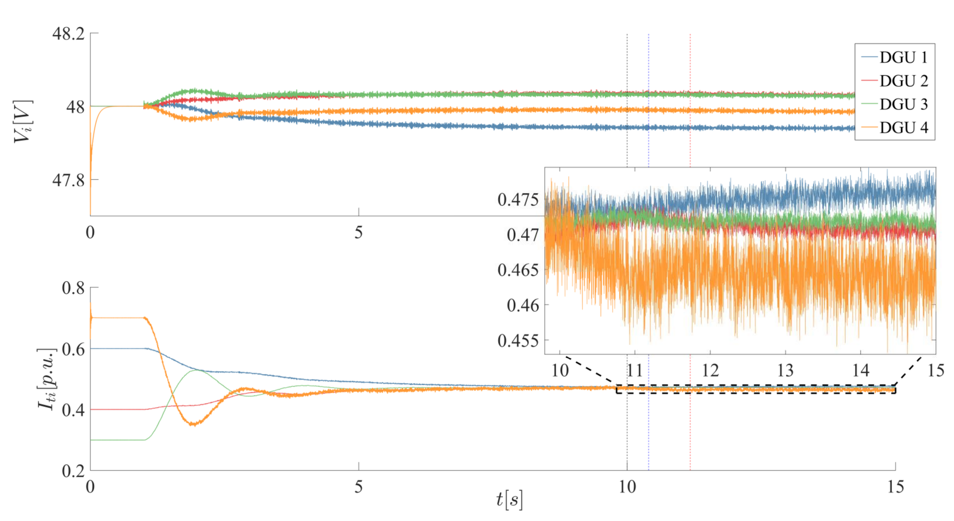
$$\left| e^{F_j(t-T_a)} H_j \phi_{j,i}(T_a) + T_j \phi_{j,i}(t) - \int_{T_a}^{t} e^{F_j(t-\tau)} \left[\widehat{K}_j \phi_{j,i}(\tau)\right] d\tau \right| = 0$$

Remark

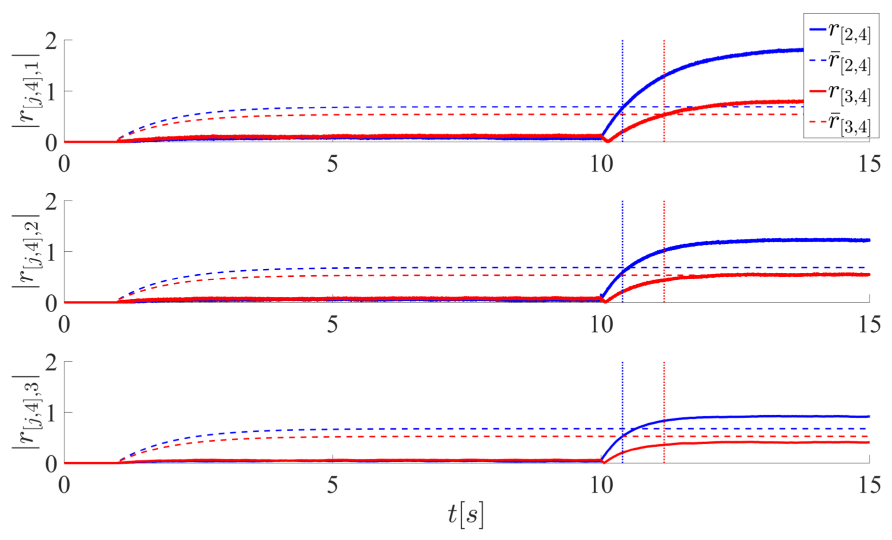
The LHS argument of both sufficient conditions corresponds to the **overall effect** that the attack has on the residual.

- Attack is guaranteed to be detectable if its effect is such to not be explainable with noise;
- Attack is stealthy if it does not have an effect on the residual error
  - ➢ Does not imply attack does not influence microgrid dynamics

Simulation Results



State trajectory under constant bias injection attack – current sharing interrupted



UIO residuals vs. thresholds Attacks detected

Future Research Directions

- Augmented detection scheme with local state estimation
- Distributed watermarking scheme for *replay attack* detection
- Realistic DGU model and communication network

Acknowledgements

The results presented here were presented at ECC 2018: A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, & G. Ferrari-Trecate "Distributed Cyber-Attack Detection in the Secondary Control of DC Microgrids". In *European Control Conference 2018*