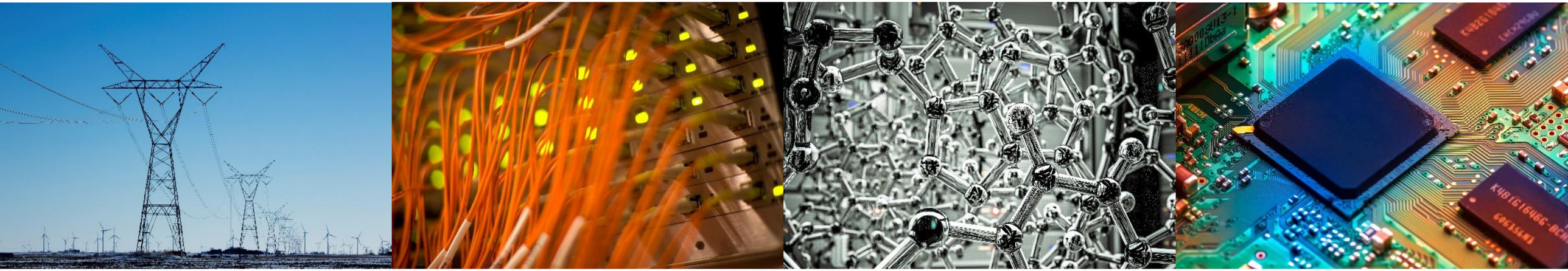
A State Estimation-Based Approach to Detect Data Integrity Threats in Combined AC-DC Power Grids

Abhiroop Chattopadhyay
Electrical and Computer Engineering, University of Illinois at Urbana-Champaign (UIUC)



In collaboration with

- Alfonso Valdes and Richard Macwan, Information Trust Institute, UIUC
- Reynaldo Nuqui, ABB Corporate Research

Work supported by the Department of Energy, DE-OE0000824

ILLINOIS
Electrical & Computer Engineering
COLLEGE OF ENGINEERING

Outline

- Introduction and Motivation
- Threats Under Consideration
- The Thrust of the Approach and Detection Criterion
- Salient Features of the Approach
- Basic Layout of Study
- Threat Modeling/Assumptions
- Simulation Methodology
- Detection Results and Conclusions

Introduction and Motivation

- **Problem:** With the increasing reliance of power system monitoring and control over communication protocols, the possibility of entities with malicious intent to gain access to and alter operational commands have become more likely.
- **One Conventional Approach:** detect whether signals may have been compromised by deploying intrusion detection/prevention techniques to examine and verify the syntax of protocol messages.
- **An Alternate Approach:** A power-systems based approach that leverages our understanding of the system's structure.

Threat Under Consideration

- The threat under consideration are data-integrity threats, that are able to bypass message envelope error checks, i.e., “syntactically correct”.
- A corruption of a control signal sent for implementation, such that the control command sent is not the same that is received.

The Thrust of the Approach

- Perform a “consistency check”.
- Consider a control action $U(t)$ that is being implemented over a period of time $\mathcal{T}$.
- Let $\widehat{U}(t)$ denote the system’s observed behavior in the same time interval.
- Then, we expect the following to be true over the course of the implementation

$$U(t) \approx \widehat{U}(t), \qquad \forall t \in \mathcal{T}.$$

- The system’s observed behavior is inferred by state estimation. **This is the state estimation-based approach being proposed.**

A Heuristic Detection Criterion

$$U(t) \approx \widehat{U}(t), \qquad \forall t \in \mathcal{T}.$$

We use a rate-of-change based error function as our means of detection.

Define the error as follows:

$$\rho(t) = \int_{t_0}^{t} |u(\tau) - \hat{u}(\tau)| d\tau, \qquad t \in \mathcal{T}$$

The detection criterion can be described as

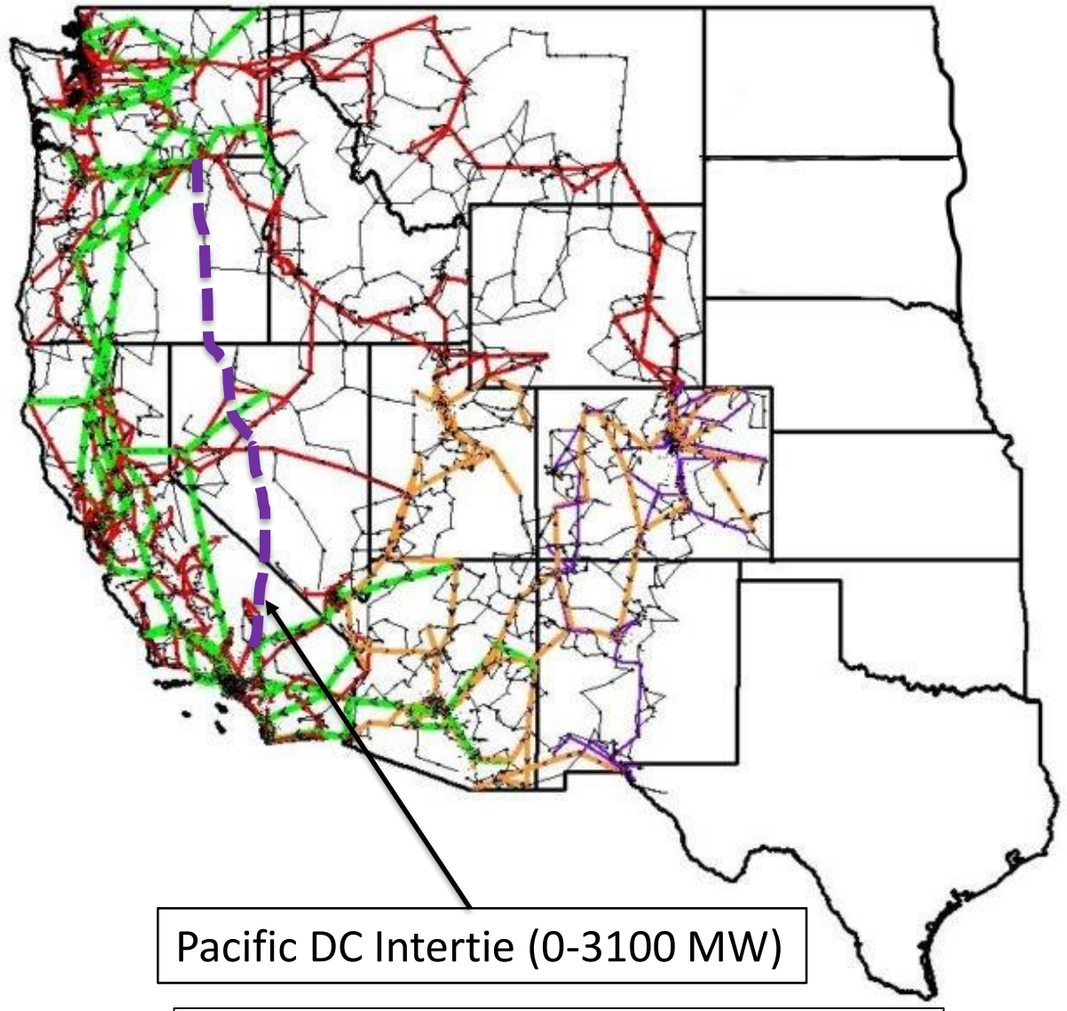
$$t^* = \min\{t \in \mathcal{T} : \rho(t) > \varepsilon\}$$

Salient Features of the Approach

- For the approach to be effective, the system's behavior should be observed with high time resolution.
- This means performing state estimation very frequently, much more so than is typically done in operations.
- To make the computation tractable under the limited time budgets, we make two approximations:
  - Prioritize a small set of measurements to receive in real-time
  - Restrict the number of iterations in the WLS state estimation computation.

Study Case

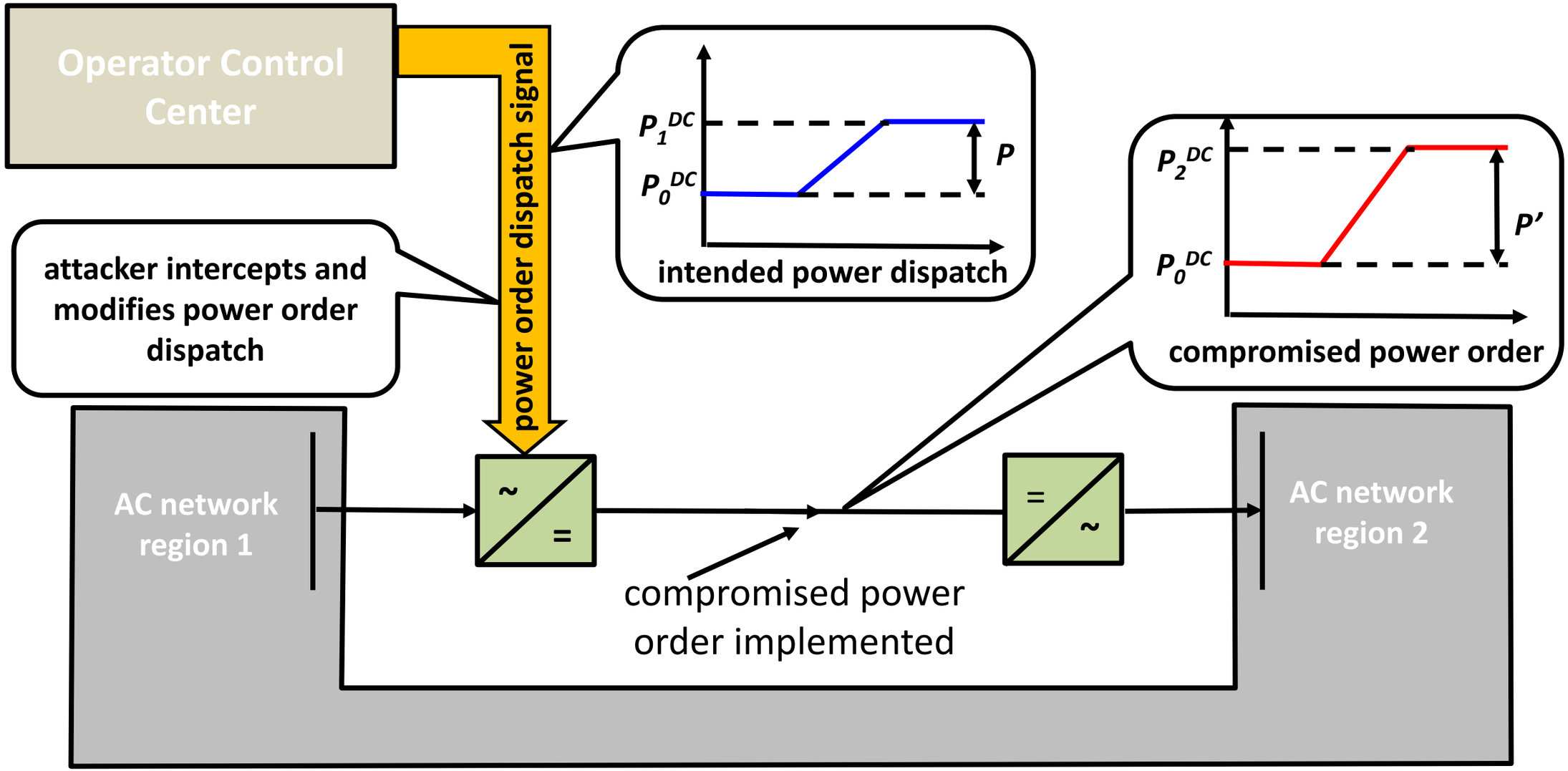
- We focus on threats that are directed at an HVDC transmission line in a combined AC-DC system.
- The case under study is a synthetic model of the transmission grid of the Western United States with the Pacific DC intertie HVDC transmission link.
- Demonstrate the effectiveness of the approach in tracking a power order.



Basic Layout of Study and Threat Modeling

- The power flow on the HVDC link is determined from the OPF solution.
- The power dispatch signal is currently communicated to the respective HVDC stations via a telecommunication link.
- All the controls at the HVDC station are local, including converter controls, AC and DC circuit breakers, etc.
- Since there is no direct control of the HVDC converter station from the control center, the indirect attacks that can be executed are investigated.
- Adversary has the capability to spoof and alter the telecommunication link of the power dispatch signal.

Graphical depiction of the threat



Premises/Assumptions

- Attacker is only able to attack the telecommunication link between the Control Center and Converter Control Station (CCS).
- Measurements from the rest of the AC system are too numerous to compromise and thus not malicious.
- Network topology does not change as the power dispatch signal is implemented.
- System is considered to be in quasi-steady state at every time instant (No dynamic regime considerations).

Simulation Methodology

- PowerWorld Simulator is used to simulate implementation of a power dispatch signal in the real power system.
- The system's real and reactive line power flows are recorded as measurements.
- These measurements are fed into a state estimation algorithm developed in MATLAB.
- The estimated state is used to compute an estimate of the power injection at the AC bus of the converter station.

Metric for Measurement Prioritization

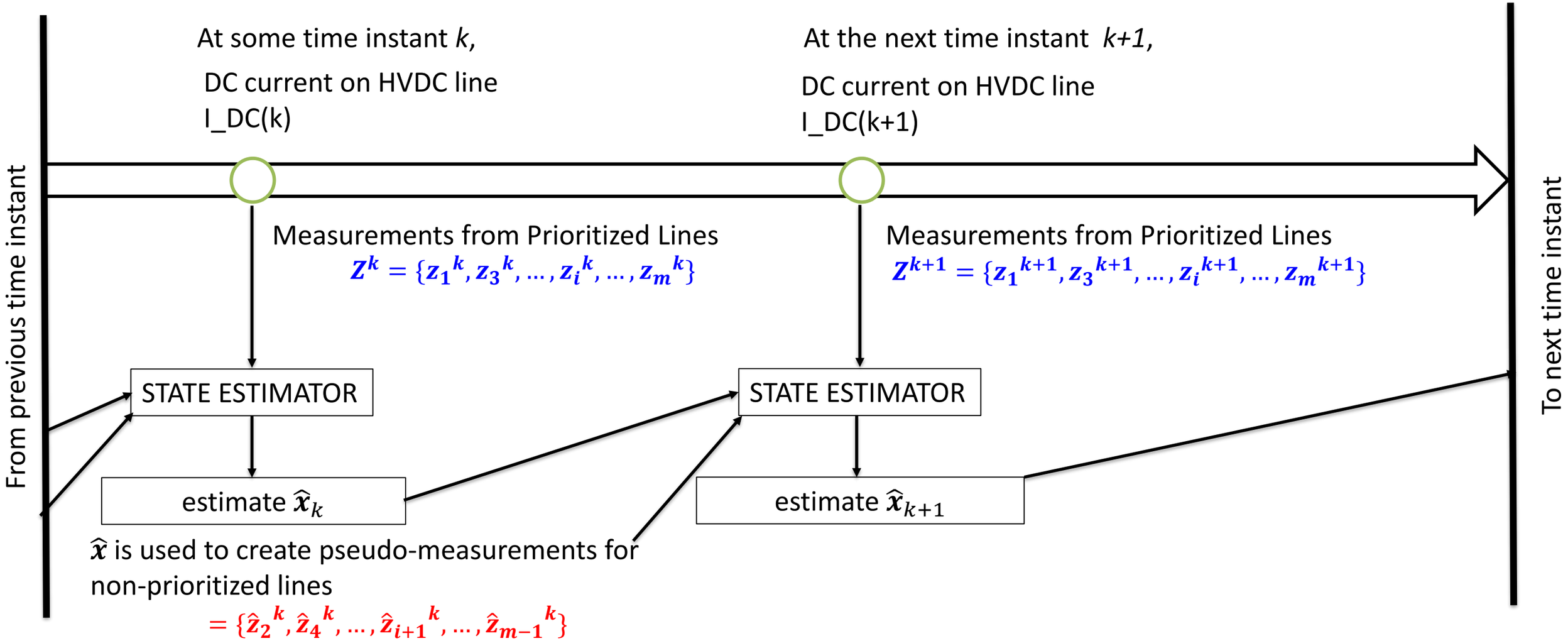
Power Transfer Distribution Factor

The PTDFs approximately quantify how MW injections at a given bus and extracted at another bus will affect the line flows on lines across the network.

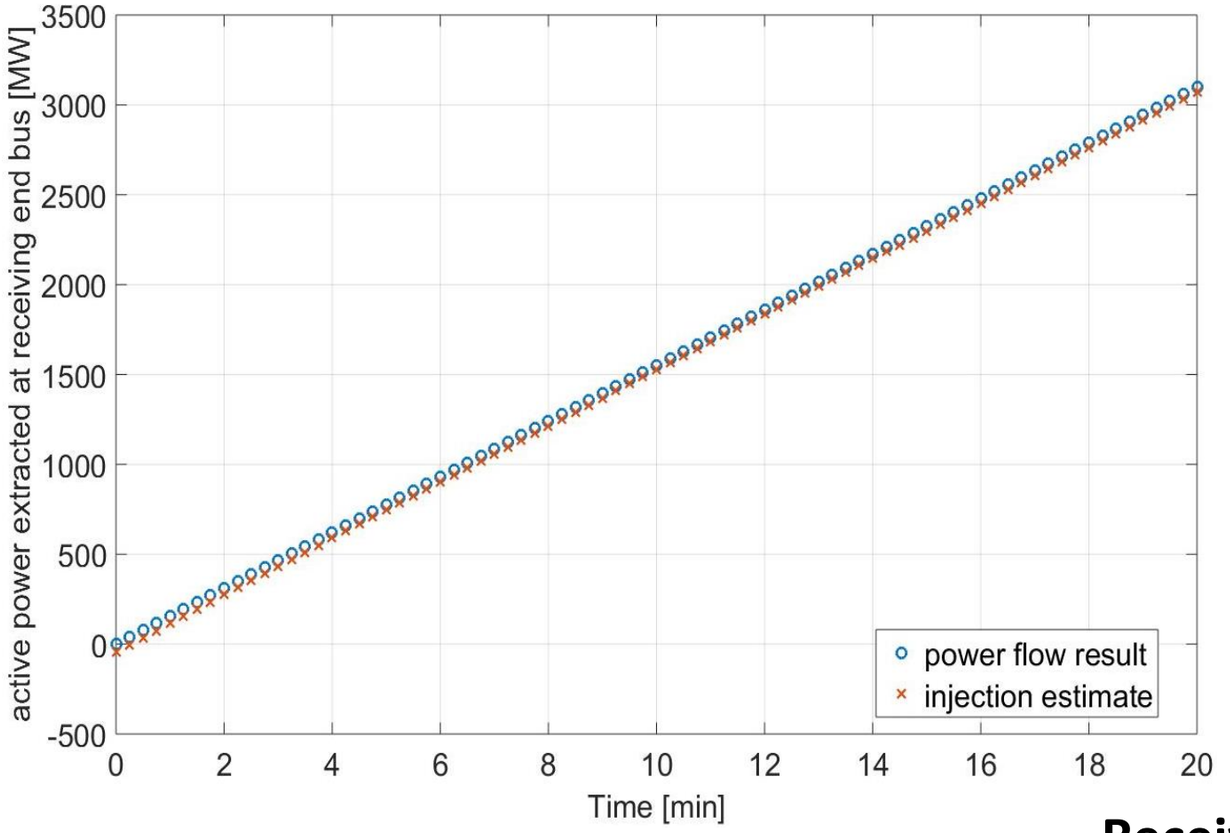
PTDF threshold $\underline{\varphi}$ [%]	Number of lines with $\varphi_l \geq \underline{\varphi}$
5	135
10	51
15	28
20	21
25	14
30	6
35	5
40	4
45	1
50	1

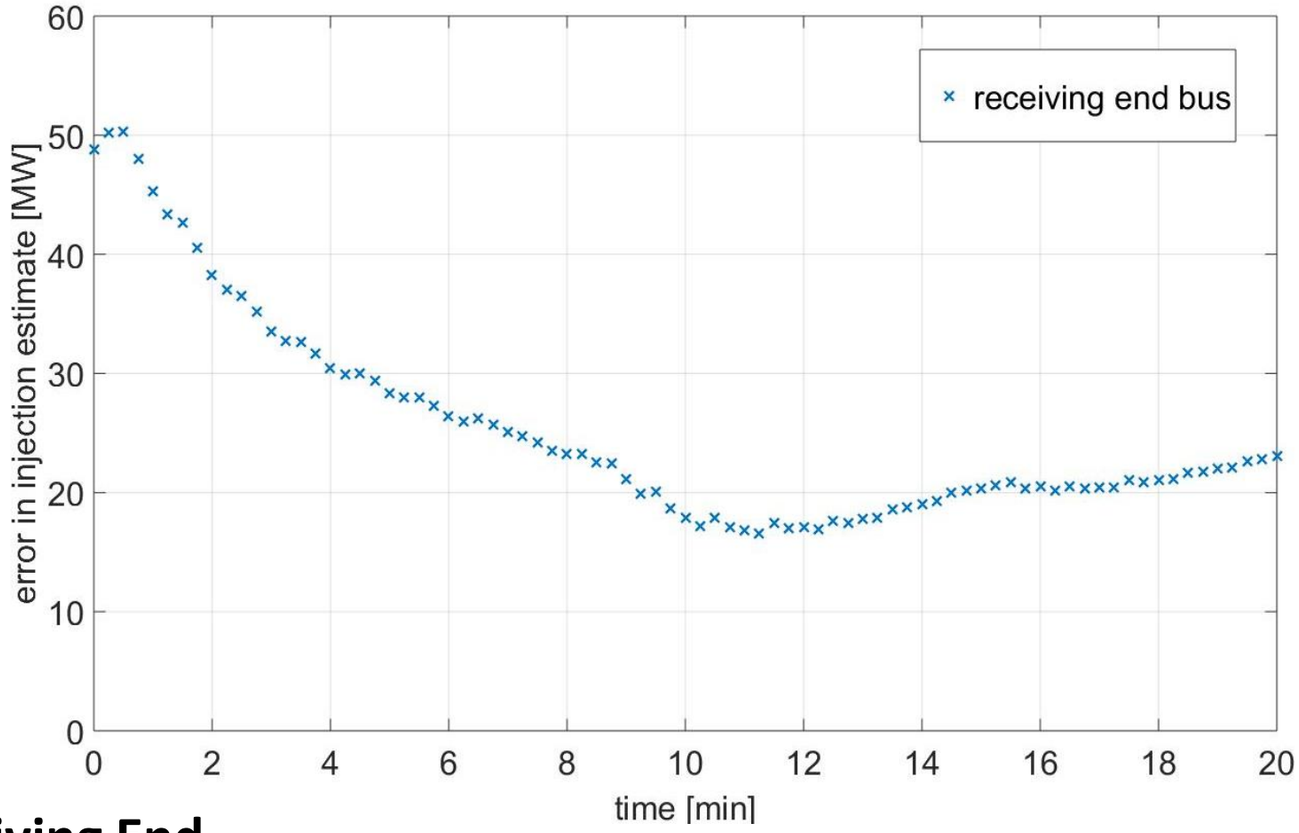
Recall system size ~ 2500 buses, 5700 lines

Graphical Depiction of the Process



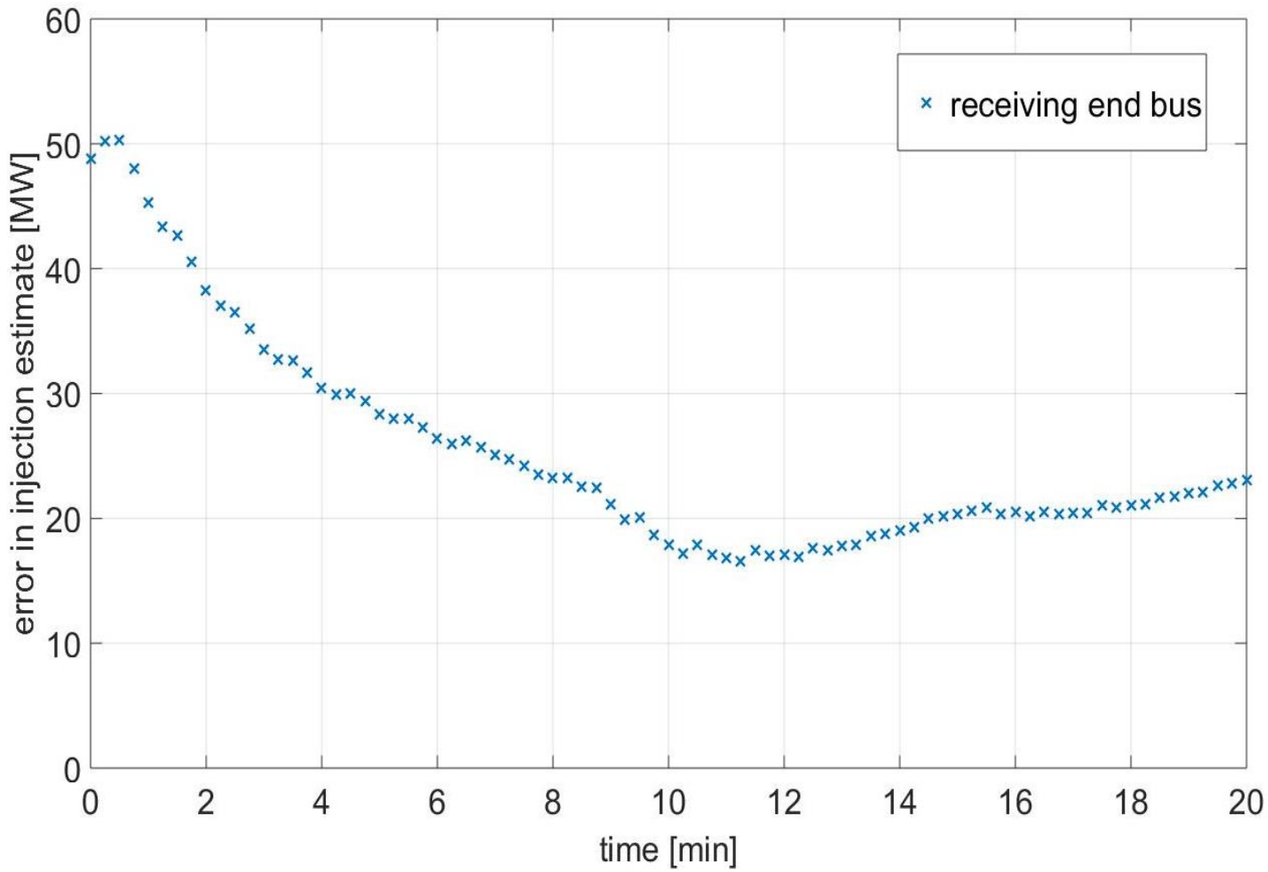
Accuracy of fast, approximate state estimator in tracking a full ramp on the HVDC line

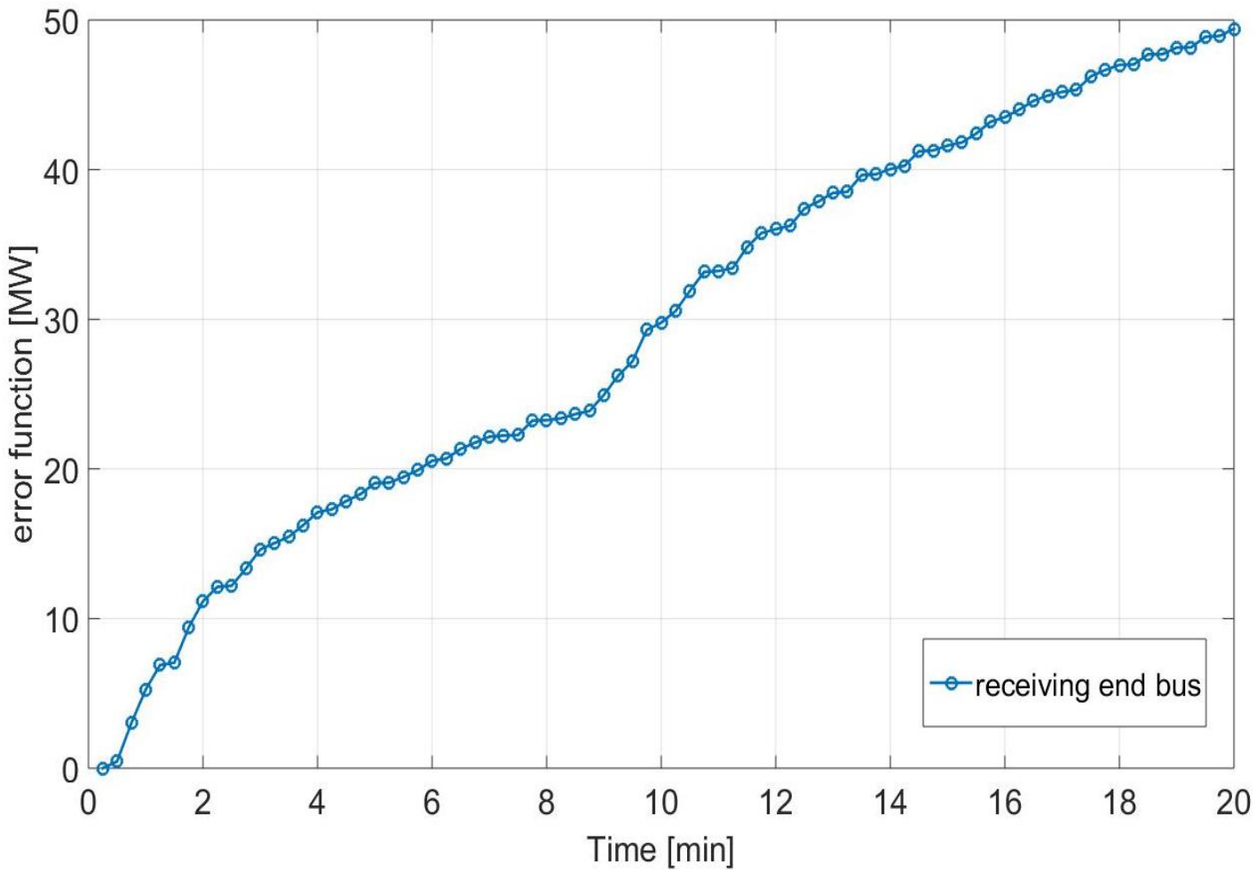




Receiving End

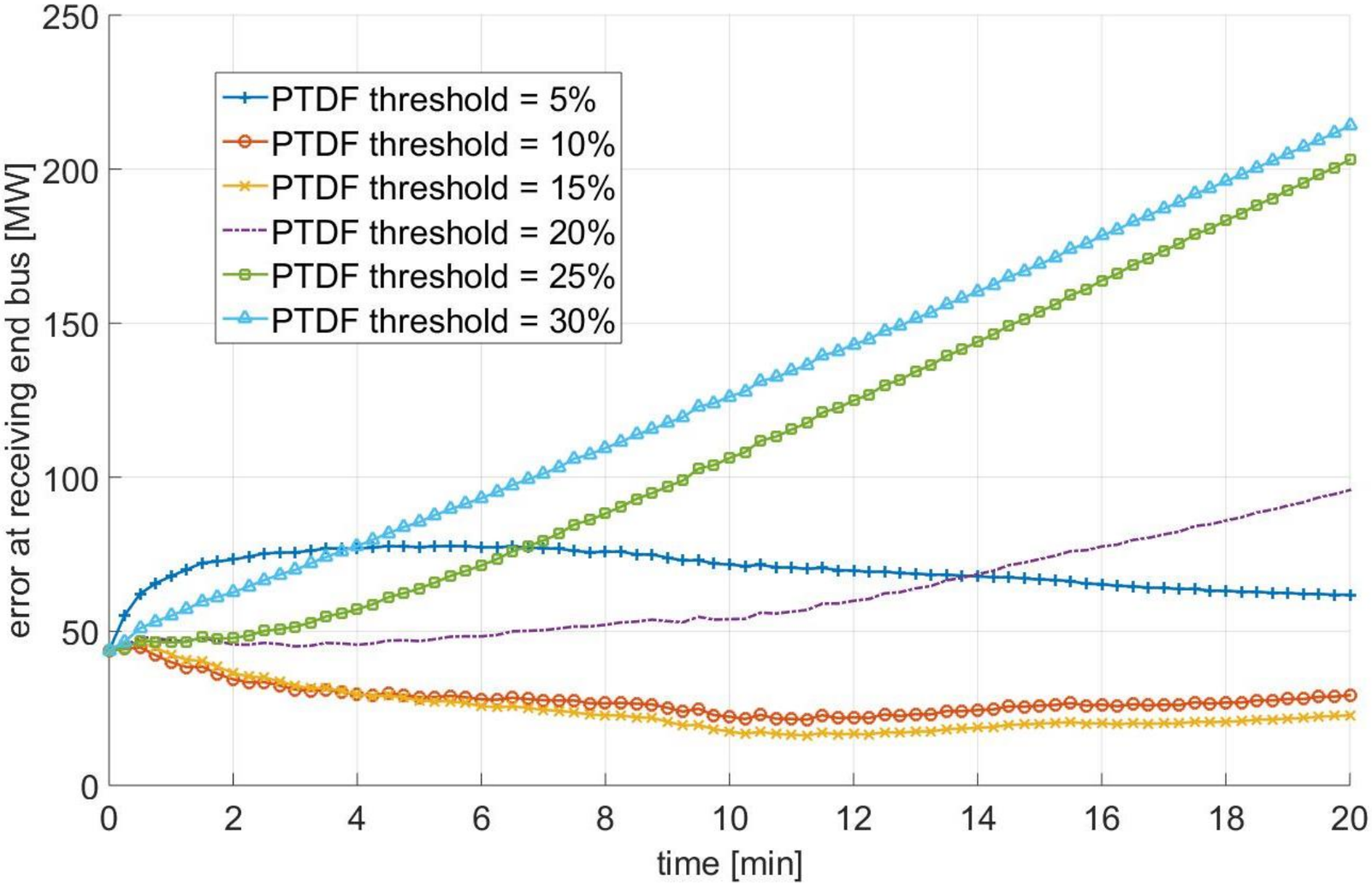
Accumulation of errors over the full ramp on the HVDC line



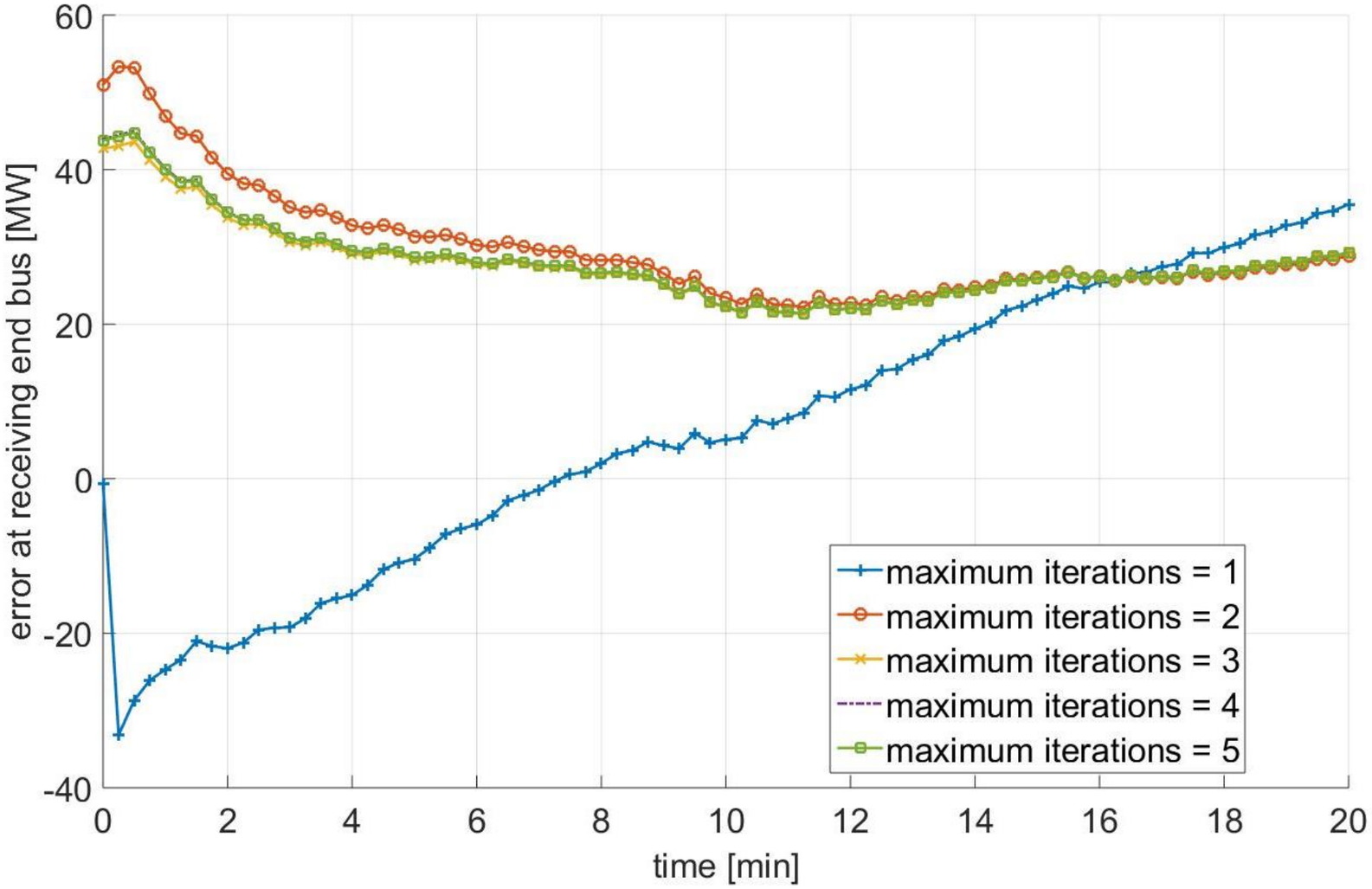


Receiving End

Sensitivity of estimates as PTDF threshold is varied

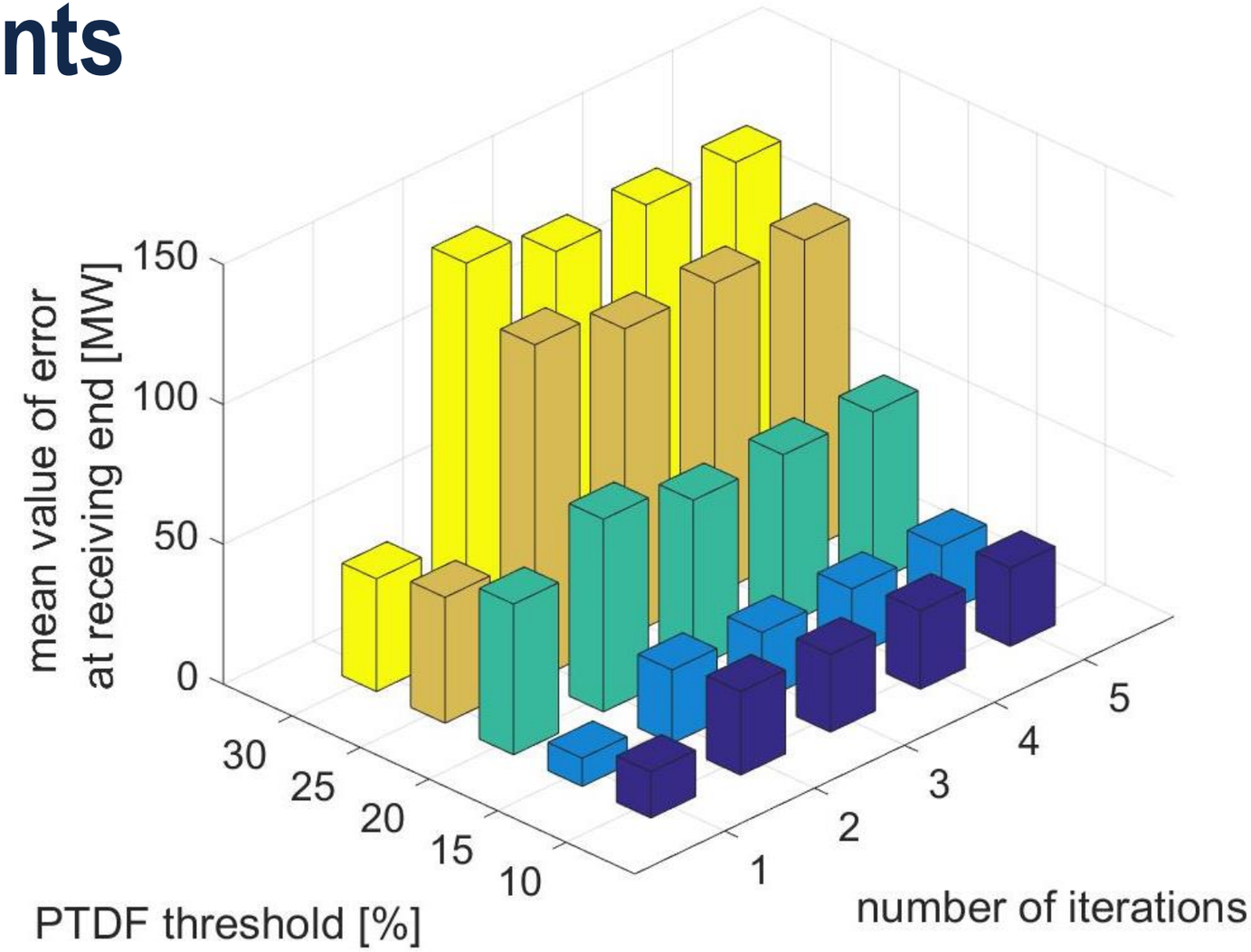


Sensitivity of estimates as max. iterations is varied

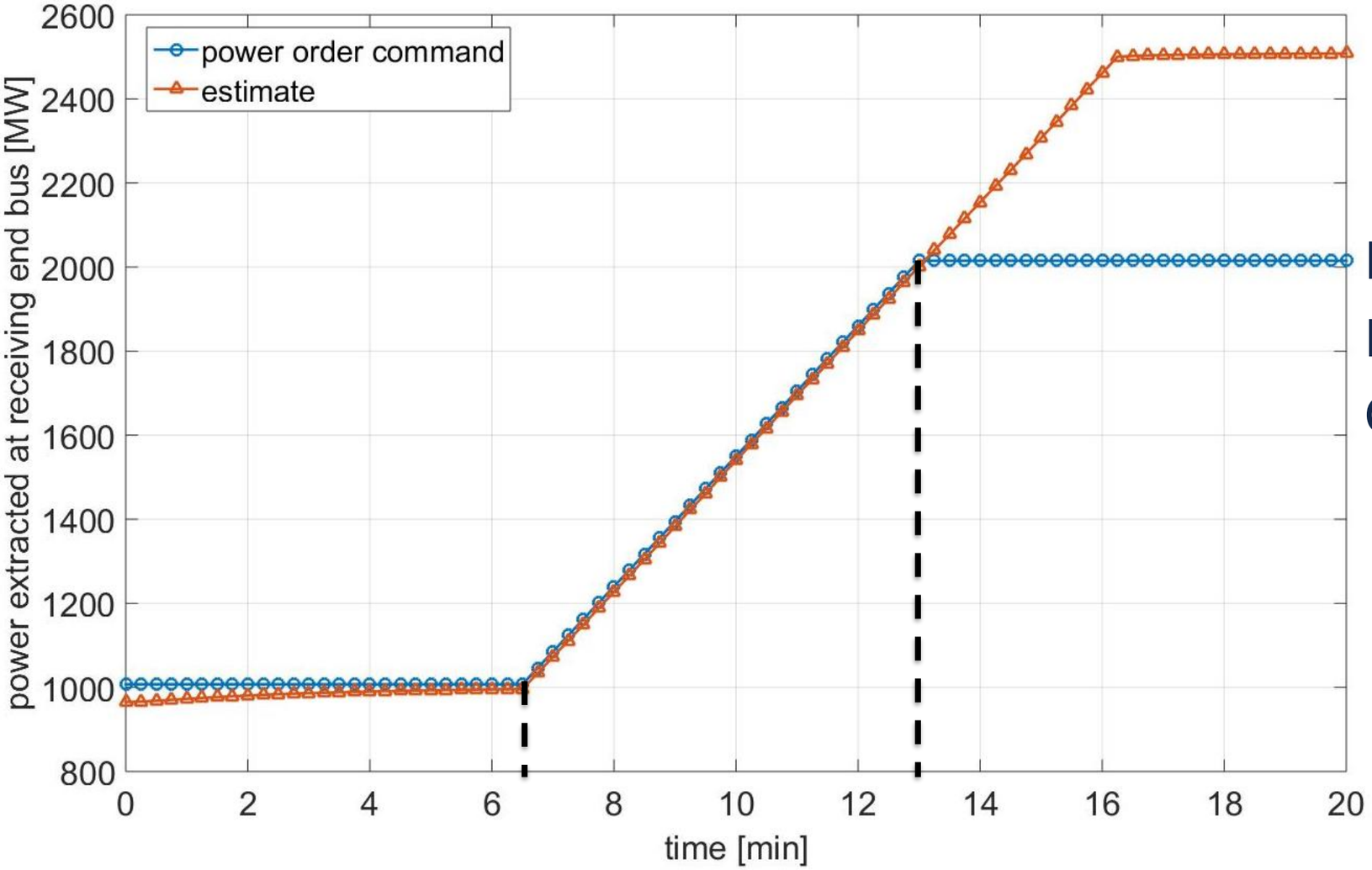


Determining optimal number of iterations and prioritized measurements

Judicious choice of maximum iterations and the number of lines to prioritize measurements from is somewhat heuristic, and specific to the case under study.



Performance of estimator under simulated threat

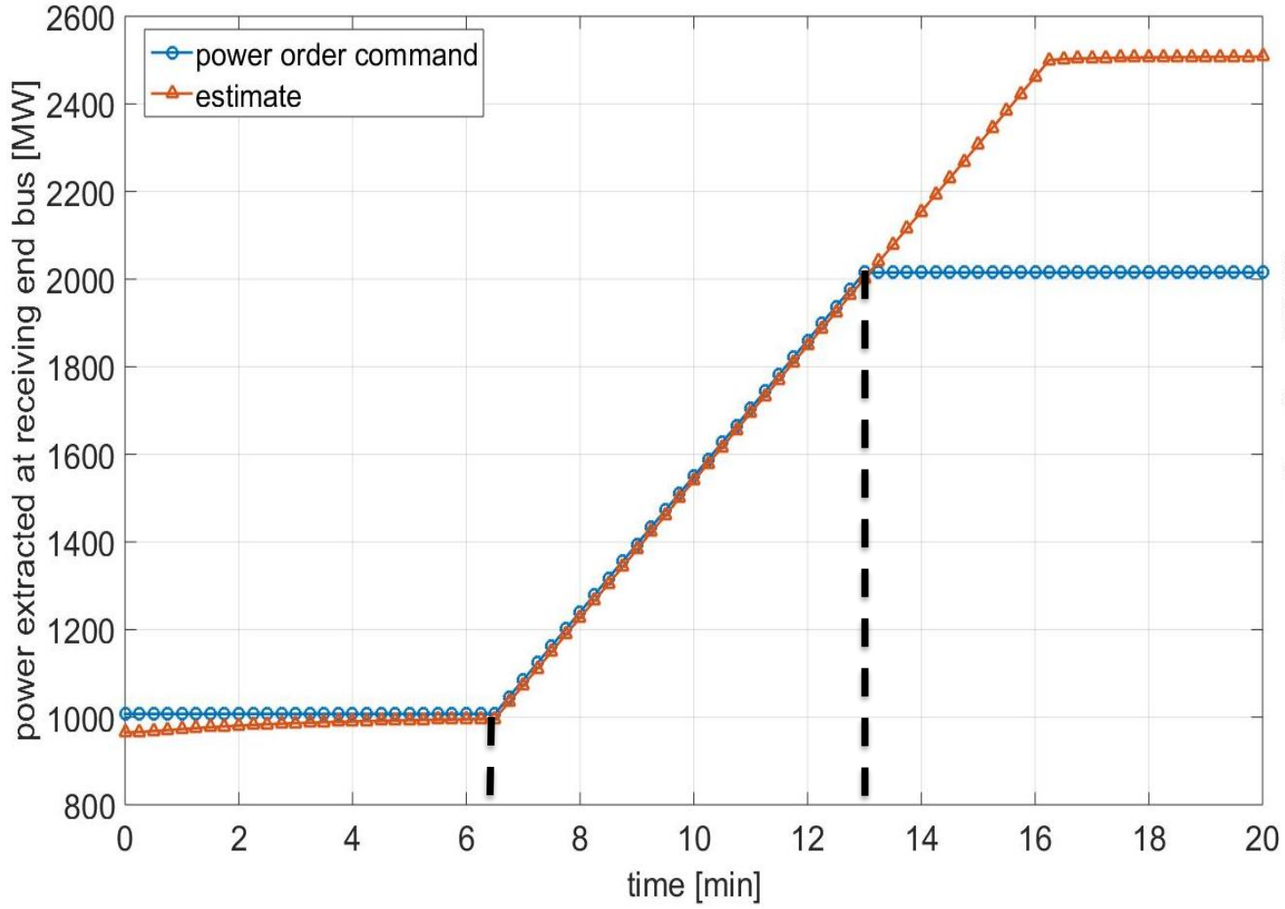


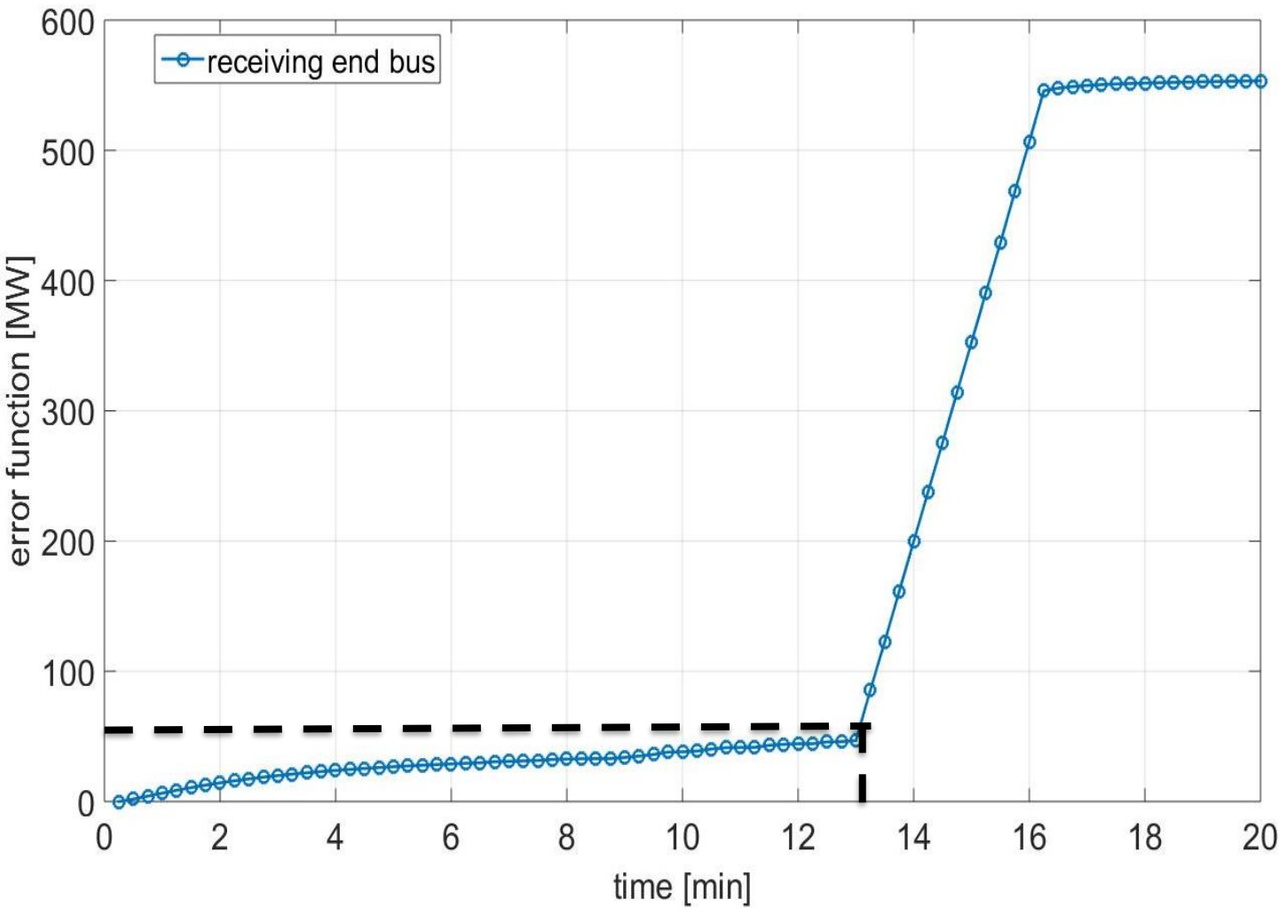
Initial value = 1000 MW,

Intended dispatch = 2000 MW,

Corrupted dispatch = 2500 MW

Error function under the simulated threat





Conclusions

- A state estimation-based approach is used as a means to track a system state's evolution over time.
- If a specific change was transmitted for implementation, then an estimate of the system state based on measurements should reflect the state variable changing as per the requested implementation.
- This approach bounds the extent to which an attacker can corrupt a implementation signal and evade detection.

Thank you!

Questions and/or comments?