Robust Overlay Networks for Microgrid Control Systems

G. Deconinck, T. Rigole, K. Vanthournout,
H. Beitollahi, R. Duan, B. Nauwelaers, E. Van Lil,
J. Driesen, R. Belmans, G. Dondossola

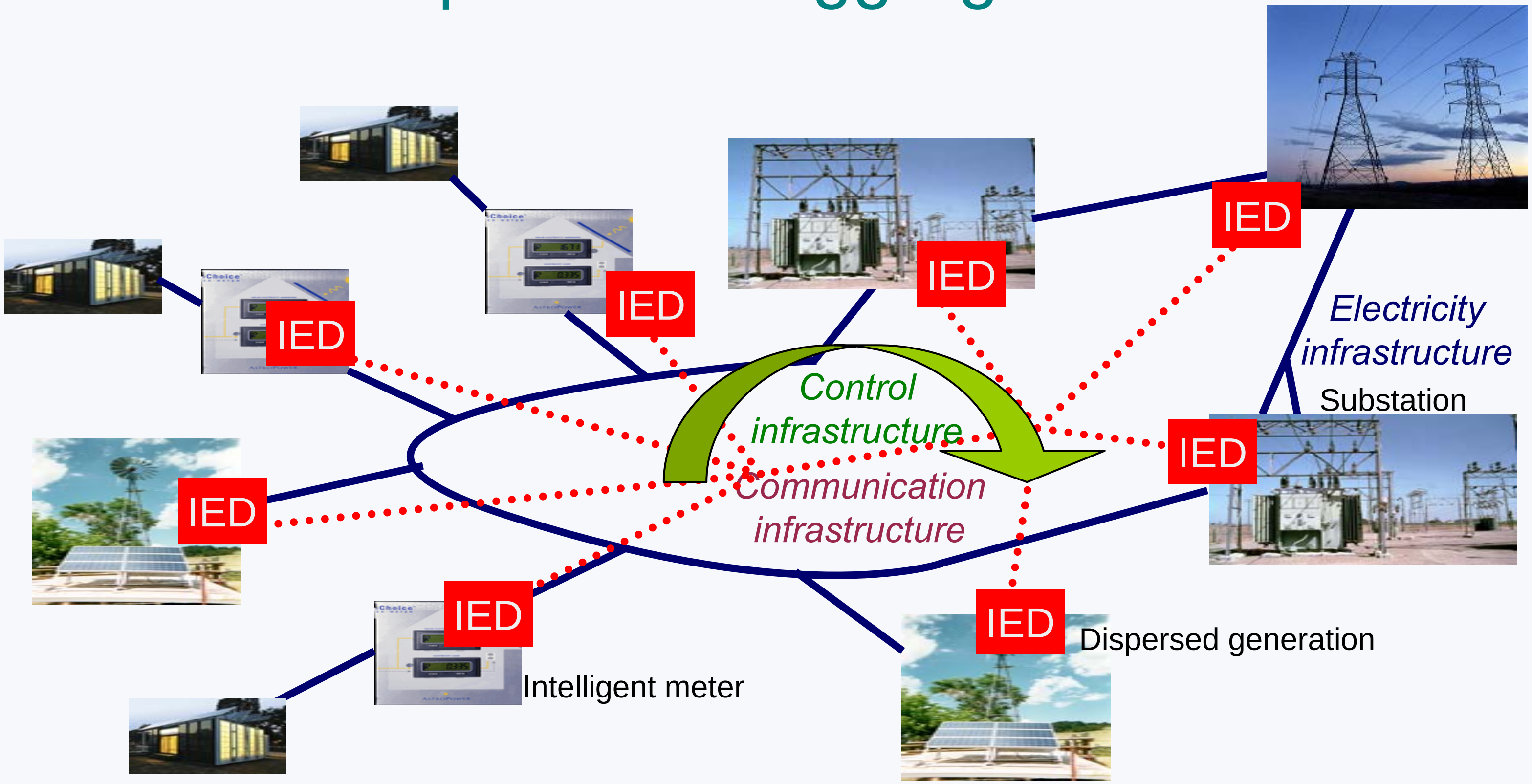
K.U.Leuven – ESAT (Belgium), CESIricerca (Italy)

WADS Edinburgh, 2007-06-27 – Critical Infrastructures

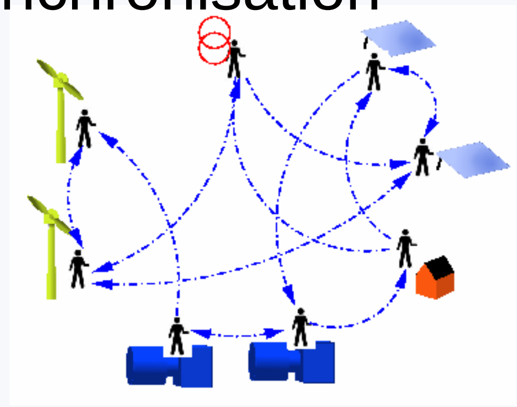
Geert.Deconinck@esat.kuleuven.be

Scope:
distributed (renewable) energy apps

- decentralised & distributed control
  - for optimising power quality, losses, costs …
  - for data acquisition & aggregation ➔ services



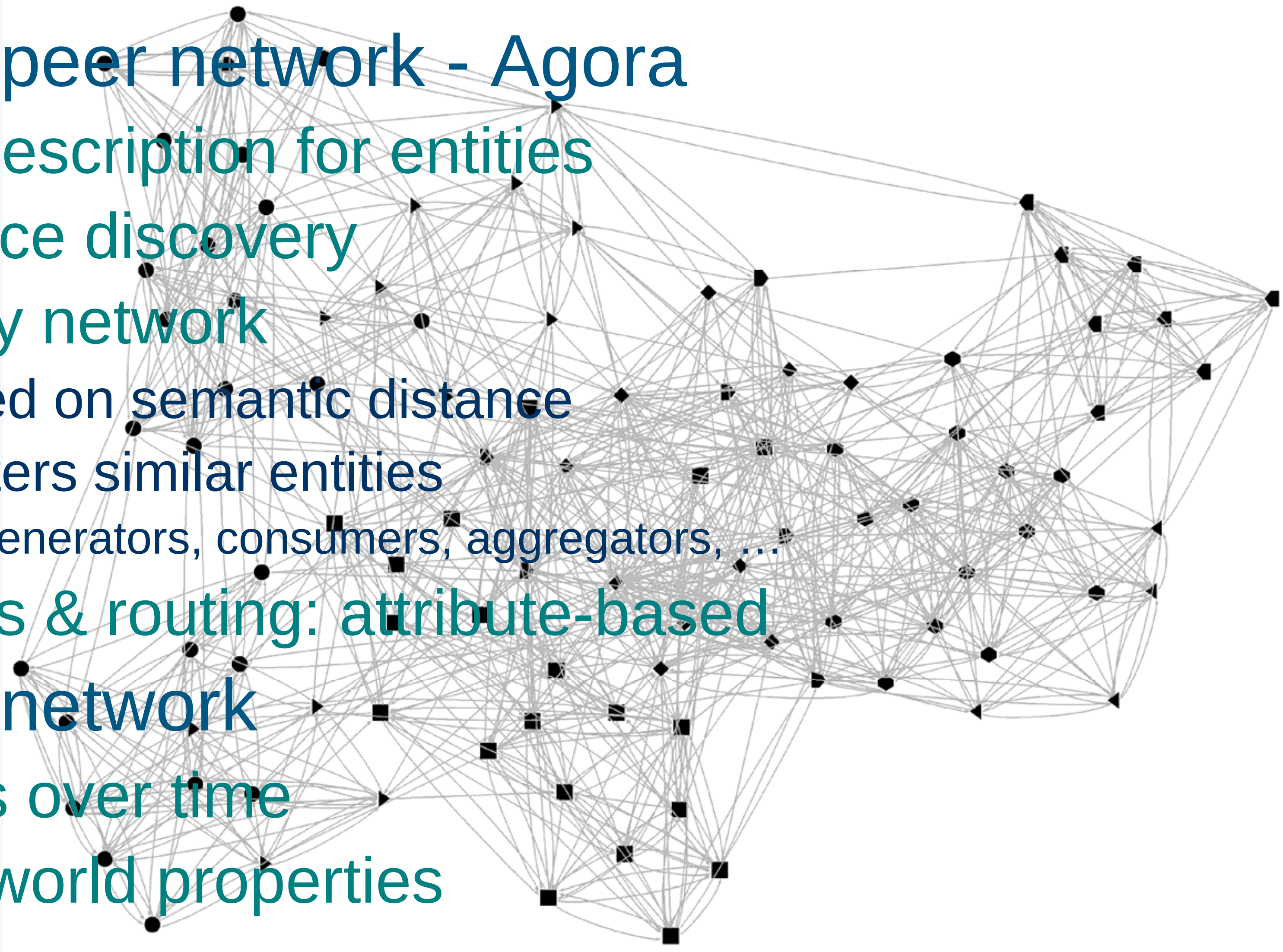
Microgrid control applications

	non real-time	*real-time*
local	data aggregation, logging	primary control (droop control)
distributed	smart metering, system monitoring, demand side mgmt, peak shaving, secondary control, tertiary control, power quality analysis, market & trading	load shedding, PQ mitigation, resynchronisation 

Control & communication infrastructure problems

- accidental faults
  - COTS components for communication and control fail
- malicious faults
  - DoS attacks on control systems via telecom backbone
  - intrusions into Centre-Substation communication flow
  - exploiting vulnerabilities in application layer protocols
  - worms or viruses
    - in substation network caused by maintenance
- need for intrusion tolerance & fault tolerance
  - in dynamic environment, based on COTS components
  - e.g. via middleware for graceful degradation

Semantic overlay network for microgrid control communication

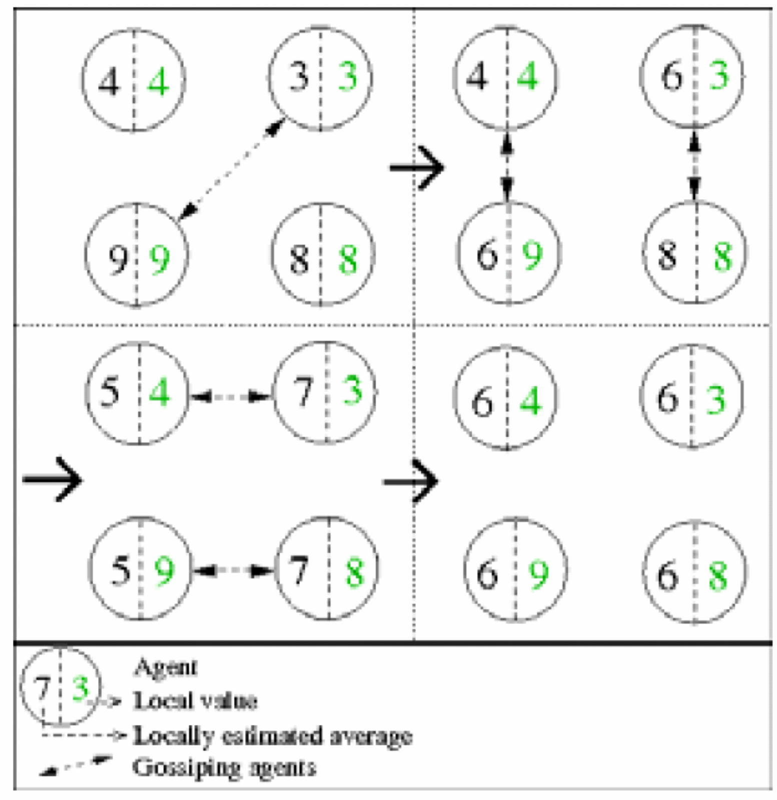


- peer-to-peer network - Agora
  - XML description for entities
  - resource discovery
  - overlay network
    - o based on semantic distance
    - o clusters similar entities
      - generators, consumers, aggregators, …
  - queries & routing: attribute-based
- overlay network
  - adapts over time
  - small world properties

Microgrid control on top of overlay network

- decentralised
- based on gossiping algorithms to spread info

IED C1	IED C2
send current average Average1→C2	send current aver Average2 → C1
receive average Average2	receive average A
calculate new average Ave.1→(Ave.1+Ave.2)/2	calculate new ave Ave.2→(Ave.2+Av



Overlay resilience against accidental and malicious faults

- based on error detection & error handling
  - periodic messages
  - reconverge overlay links
- accidental fault resilience
  - 10+% node failures without significant influence on
    - overlay's regularity and small diameter or before partitioning
  - no single points of failure
  - built to deal with dynamic environments
    - new/leaving nodes, changing functionality / resource availability, …
- less robust against targeted, malicious attacks

ICT threat assessment

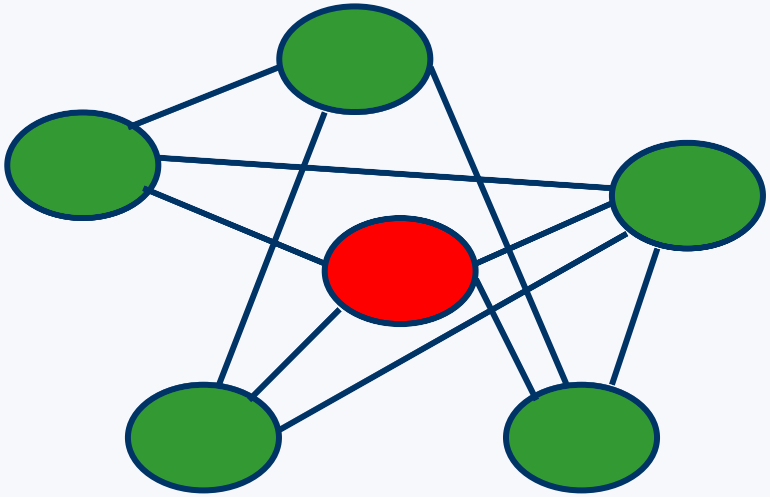
- accidental fault scenarios
  - network delays/packet loss

    → *slower convergence of 2nd-ary / 3rd-ary control loops*
  - communication failure; soft-/hardware crash

    → *overlay network can manage dynamism*
- malicious fault scenarios
  - denial-of-service attacks → *similar, not critical*
  - generic intrusions on control PCs
    - attacks on middleware level → *critical*
      - e.g. influence overlay topology
    - attacks at application level→ *critical*
      - e.g. tampering with *3rd-ary* control (financial gain)
      - e.g. tampering with *2nd-ary* control (voltage profile disturbance)

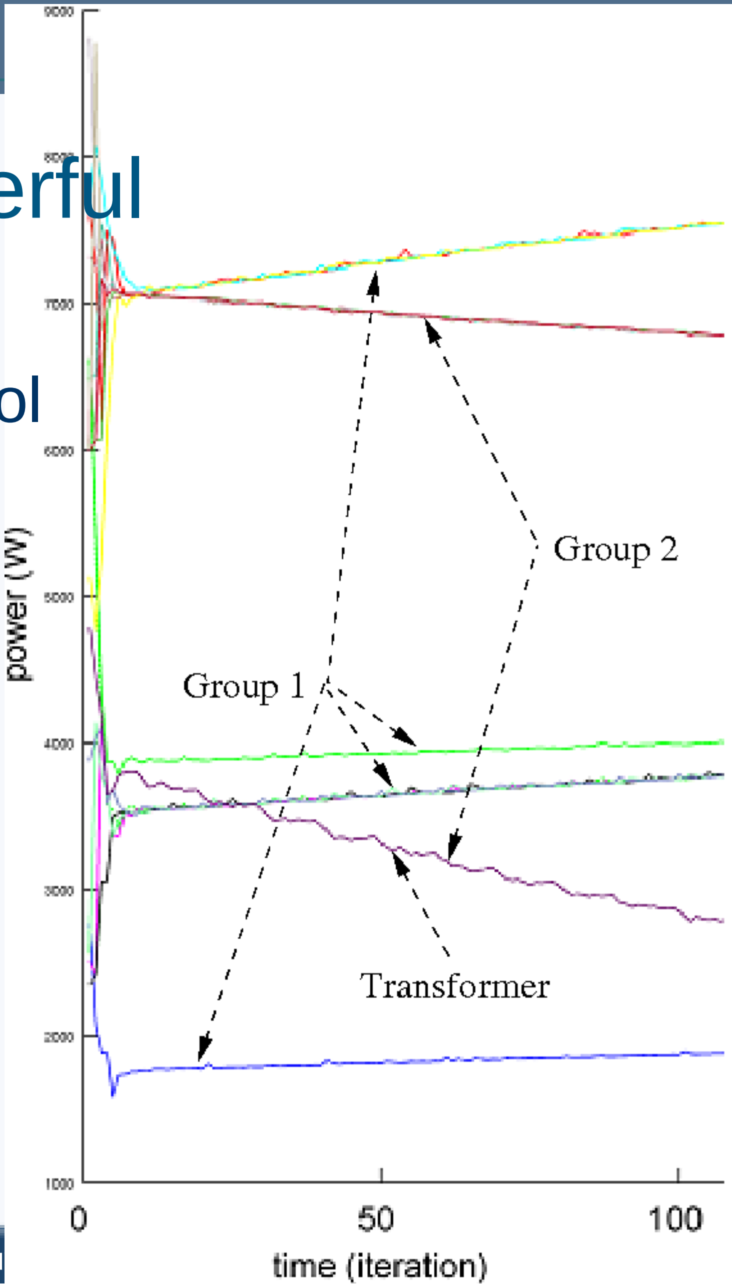
Example: overlay topology attack

- overlay networks dynamically constructed
  - here: neighbour choice based on node description
- malicious node send wrong descriptions
  - other nodes choose it as a direct neighbour



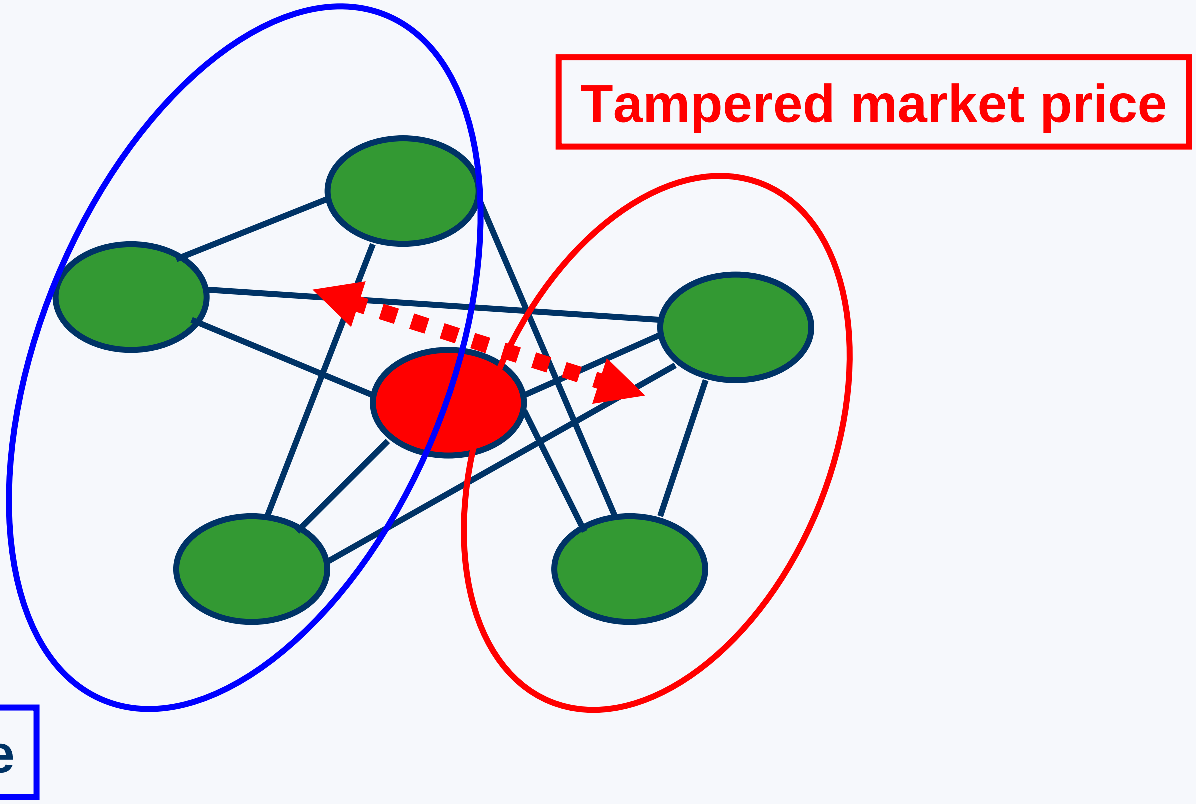
Overlay topology attack (2)

- malicious node more powerful
  - e.g. network partitioning
    - disable 2nd-ary / 3rd-ary control
    - non optimal behaviour



Overlay topology attack (3)

- malicious node more powerful
  - e.g. ‘man-in-the-middle’ economical attack



Tampered market price

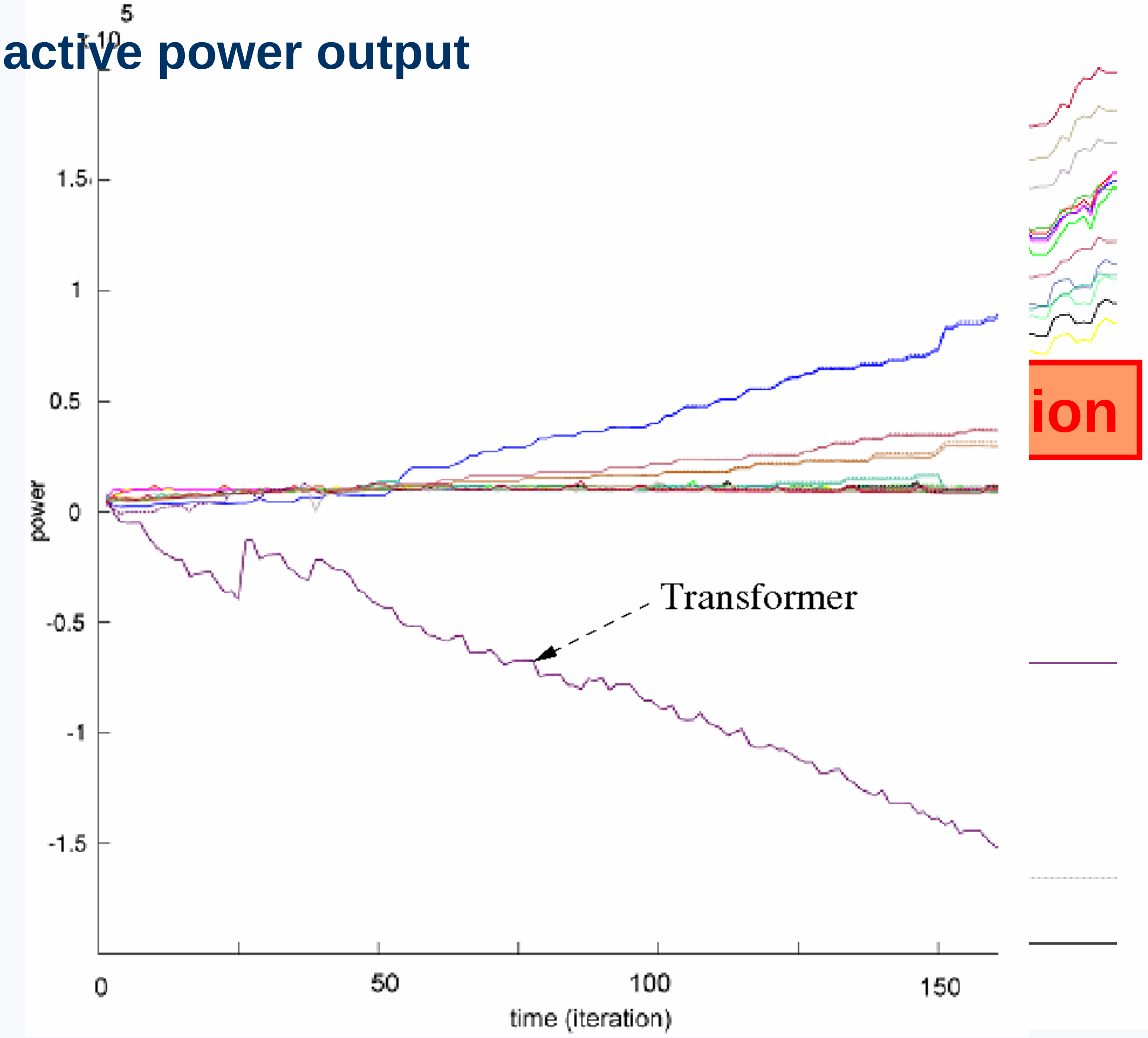
True market price

Other example scenario: secondary control attack (1)

- secondary control
  - = voltage profile management
- uses distributed averaging primitive
  - = averages system-wide divergence from optimal voltage level
- malicious node injecting false values
  - false values aggregate
  - leading to system wide power output increase

Secondary Control Attack (2)

DG increasing active power output



Conclusion

- context
  - new threats and vulnerabilities emerge from tight coupling of power - info infrastructures and from evolving control
- vision
  - resilient power control *in spite of* these threats
- approach
  - configurable middleware for improved resilience
  - methodology for modelling fault propagation & interdependencies
- projects
  - crutial.cesiricerca.it
  - www.kuleuven.be/esat/electa