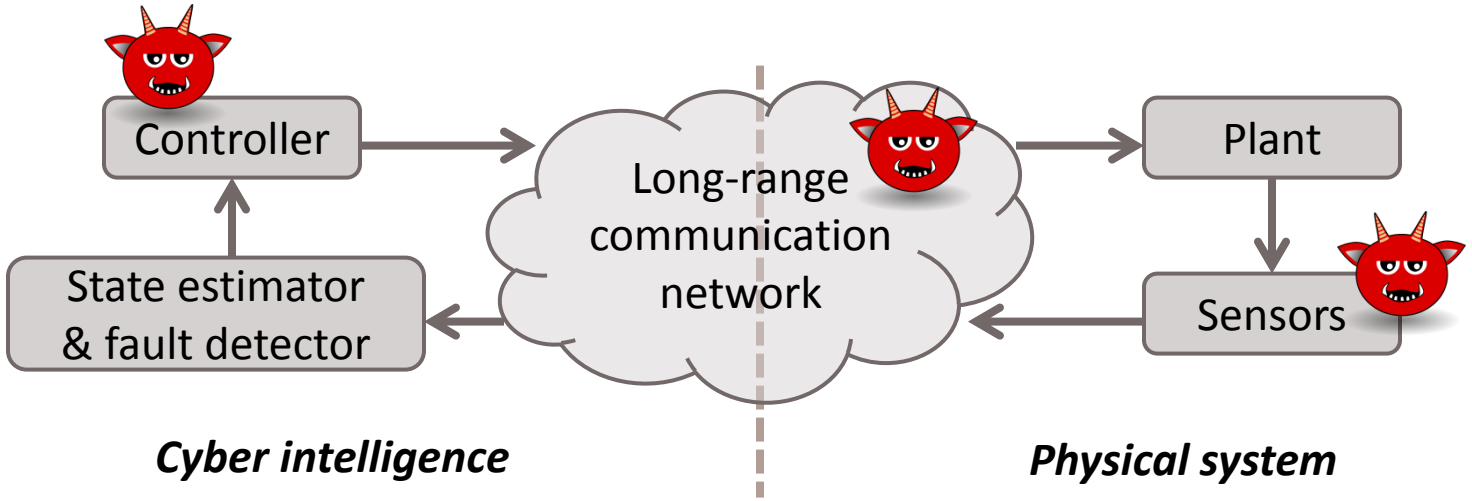
Data Integrity Attacks against Power Grid Control Systems

Rui Tan

School of Computer Science and Engineering, NTU
Advanced Digital Sciences Center, Illinois at Singapore

Threats against CPS Control



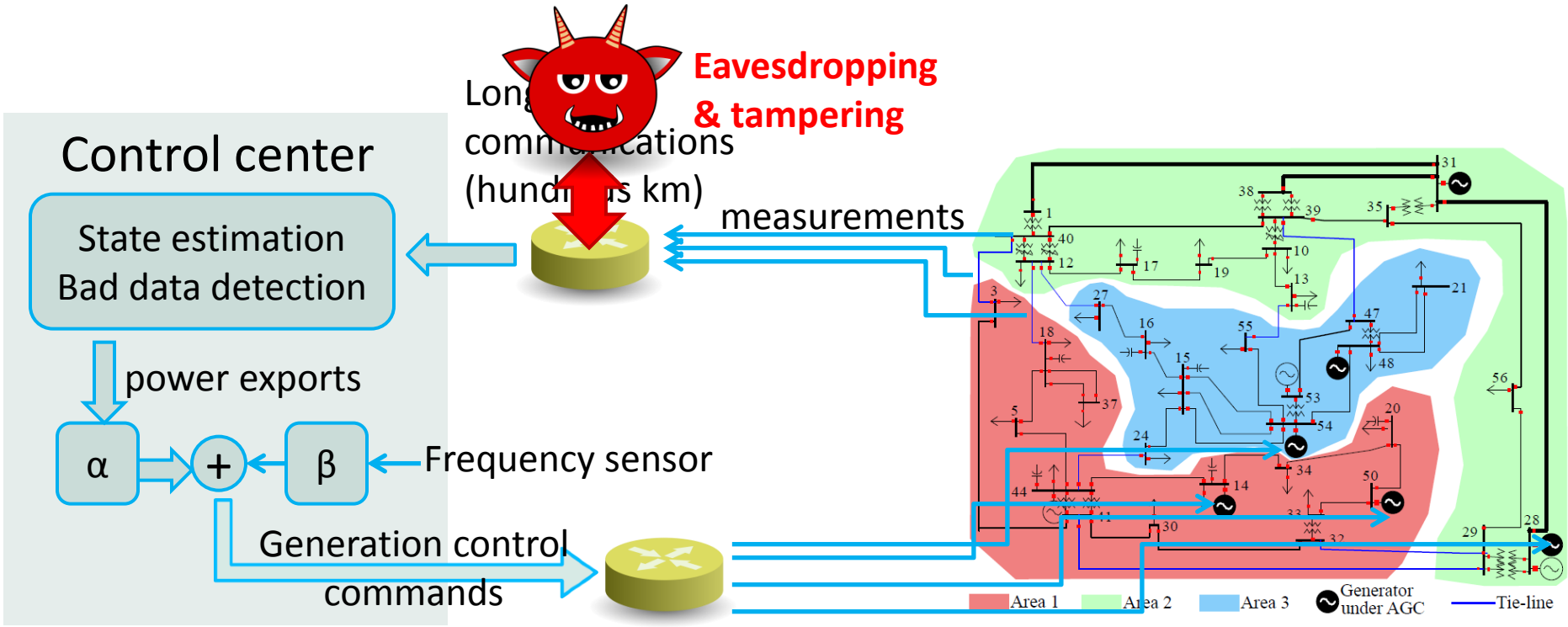
- Attacks on controllers
  - Zero-day vulnerability (Stuxnet)
  - Stepping stone attack (Dragonfly)
  - Insider (water system contamination in 2010)
- Attacks on sensors
  - Physical attack, wireless injection, GPS spoofing
- Attacks on communications
  - Heartbleed, NTP attacks, etc

Challenges and Scope

- Challenges
  - Simple attack ineffective: feedback corrects errors
  - Analysis non-trivial: complex system dynamics

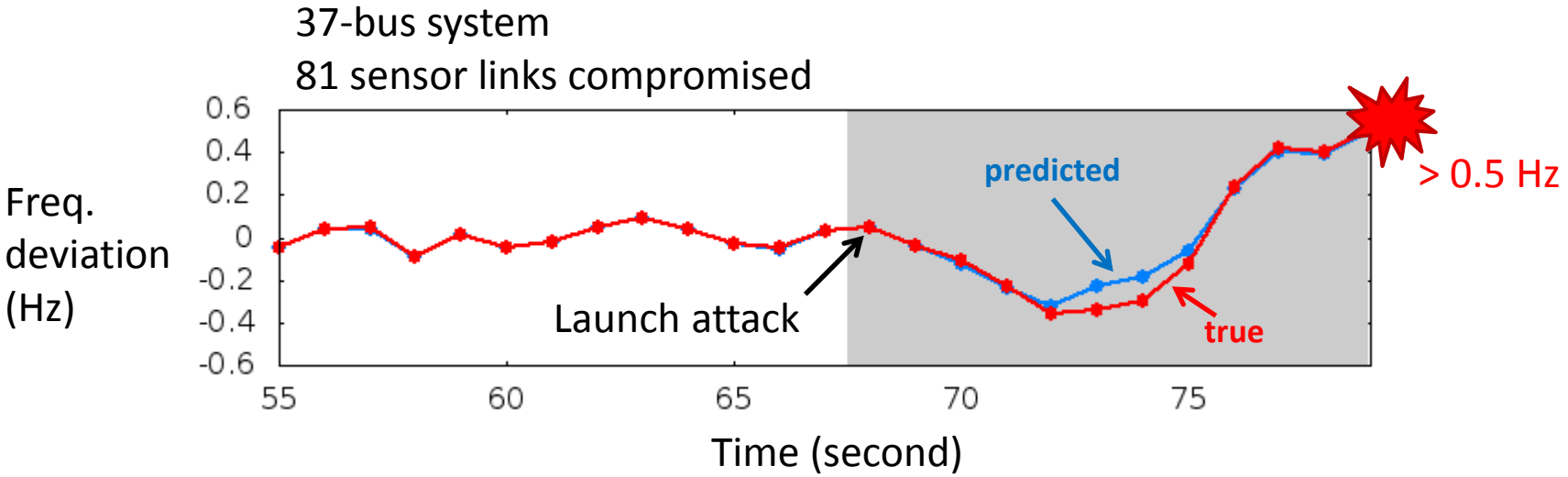
- Scope of our work
  - False data injection (FDI) against frequency control
  - Delay attack against voltage control
  - On applying fault detector against FDI
  - FDI against demand response systems

FDI against Frequency Control



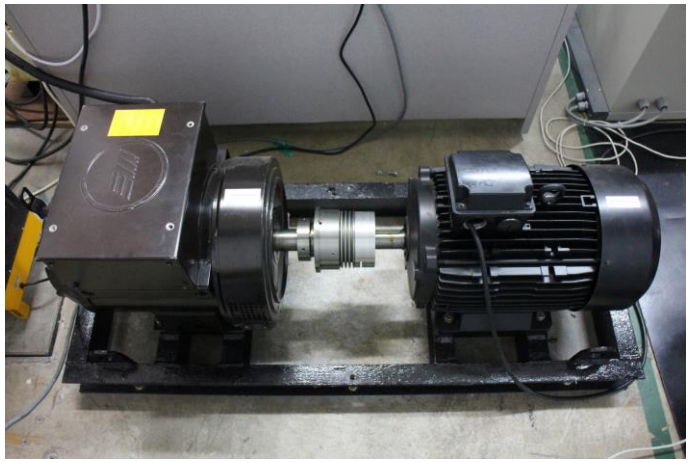
Tamper with sensor data to disturb grid frequency without being detected by existing mechanisms

Results



- Attacker
  - **Attack impact model learning** based on eavesdropped data in normal state
  - **Optimal attack** that minimizes time-to-emergency
- Defender
  - **Quick attack detection** (4 seconds)
  - **Attack identification** locates attacks

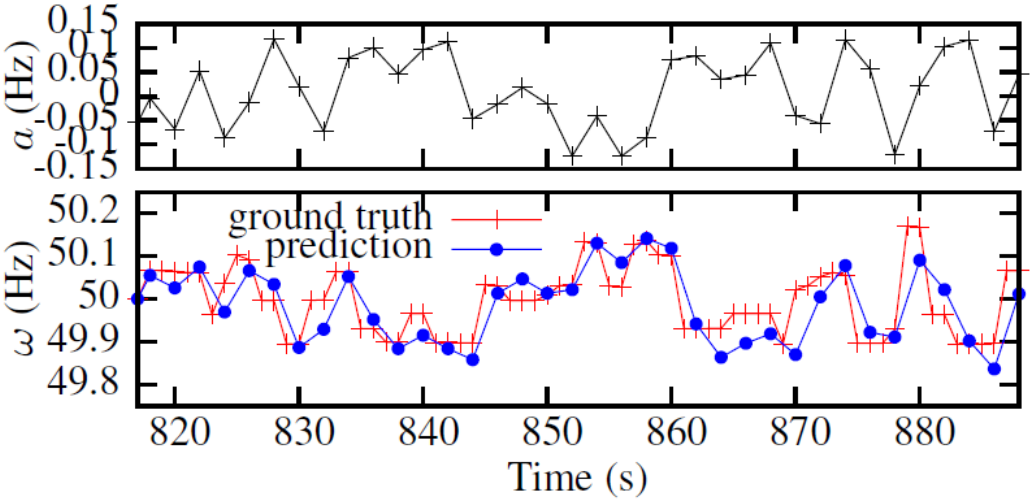
NTU Microgrid Experiment



13.5kVA generator

16-bus 400V grid

variable load

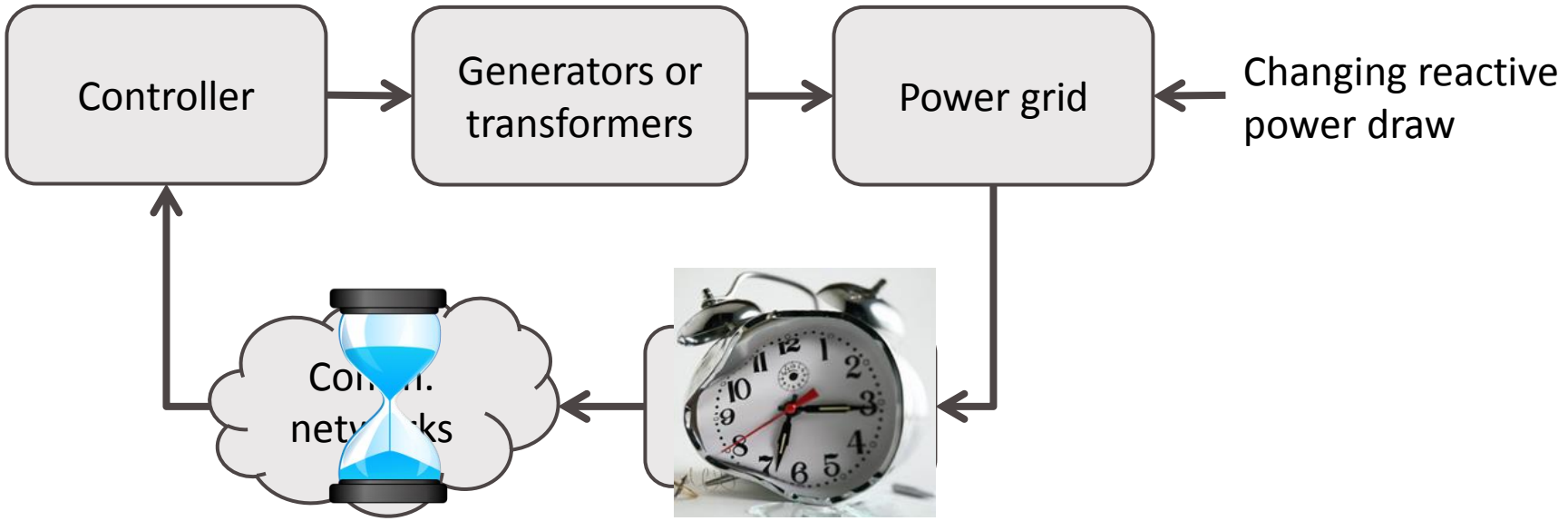


Accuracy of learned model

Achieve unsafe freq. deviation (0.5Hz) within 30 seconds

Optimal false data injection attack against automatic generation control in power grids. R. Tan, H. H. Nguyen, E.Y.S. Foo, X. Dong, D.K.Y. Yau, Z. Kalbarczyk, R. Iyer, H.B. Gooi. ICCPS 2016.

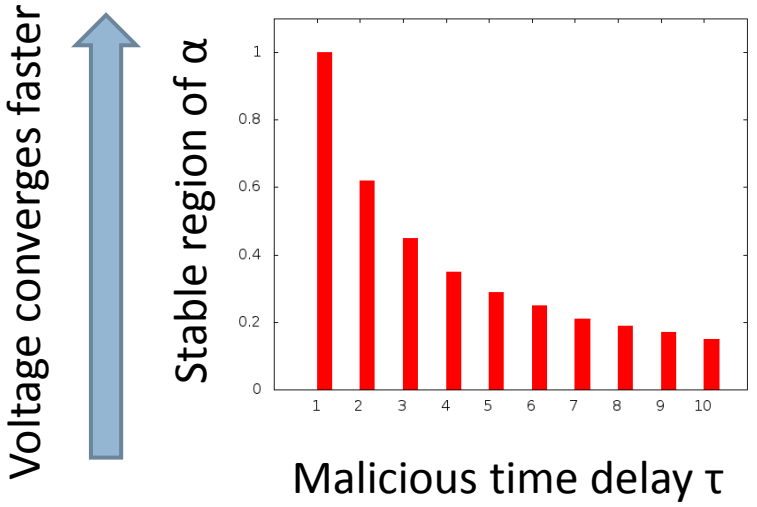
Delay Attack against Voltage Control

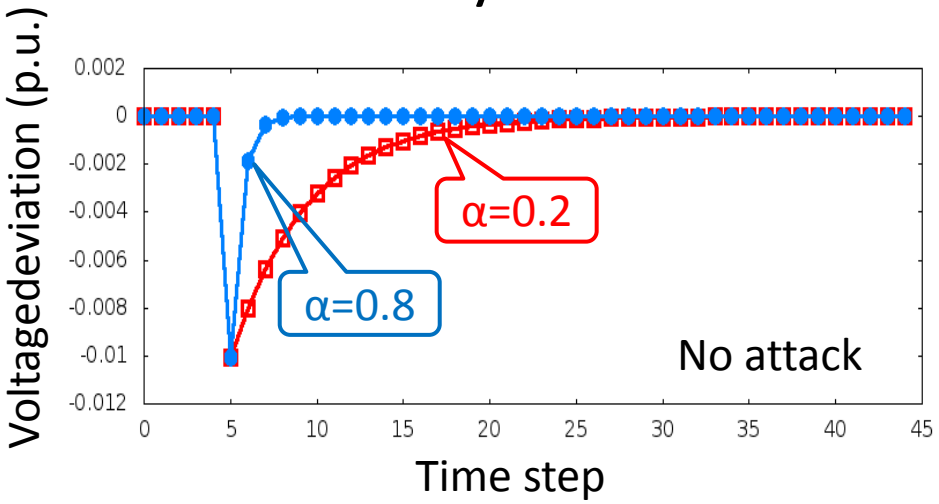


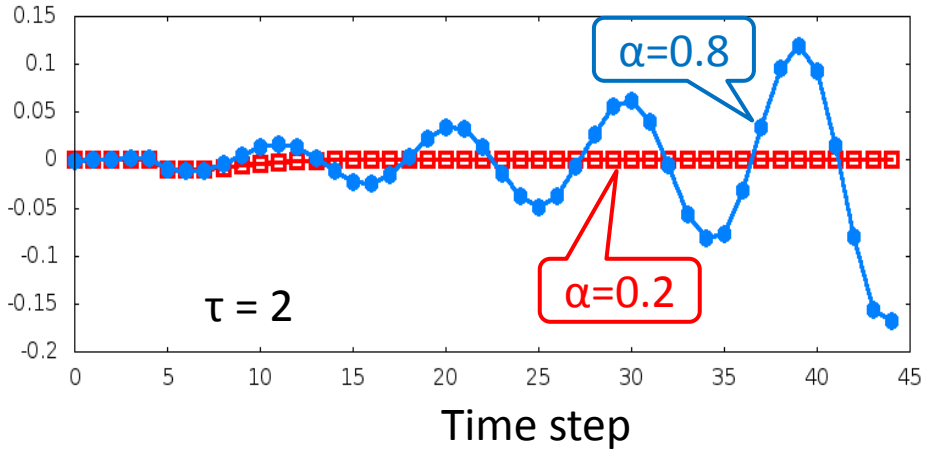
- Secondary voltage control $\mathbf{u}[n] = \alpha\mathbf{C}(\mathbf{x}_0 - \mathbf{x}[n])$
  - Used in power grids
- Delay attack $\mathbf{u}[n] = \alpha\mathbf{C}(\mathbf{x}_0 - \mathbf{x}[n - \tau])$
  - Network congestion, time desynchronization, etc

Results

- Trade-off
  - Voltage convergence speed
  - Tolerable malicious delay
- PowerWorld simulations
  - 37-bus system



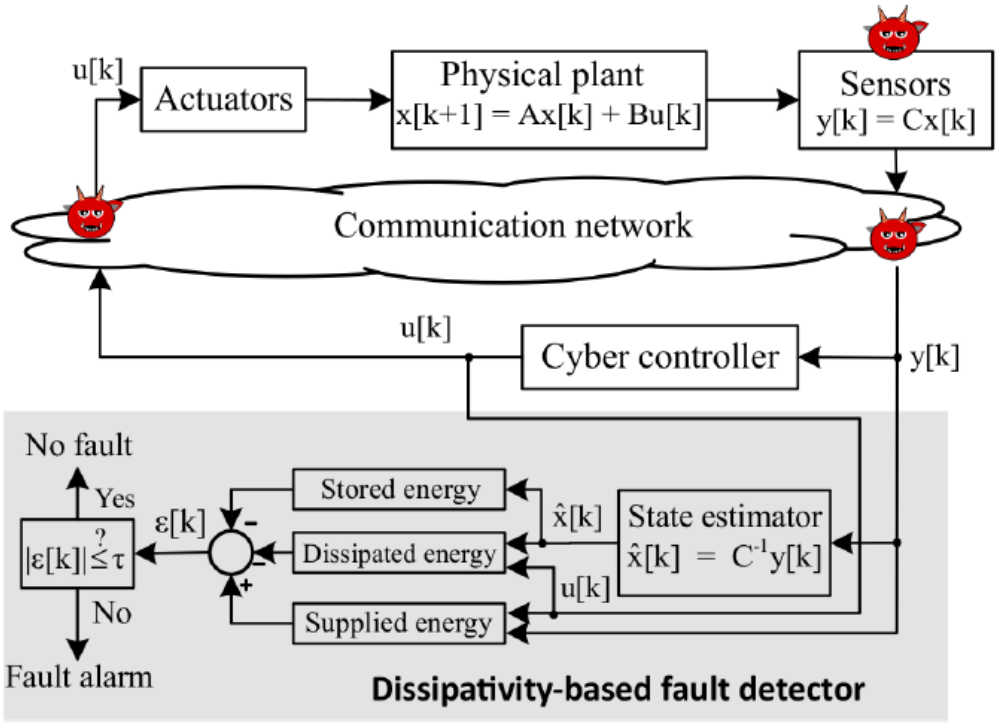




Impact of Signal Delay Attack on Voltage Control for Electrified Railways.
H. H. Nguyen, R. Tan, D.Y.K. Yau. IEEE TENCON'15.

Is Fault Detector Enough?

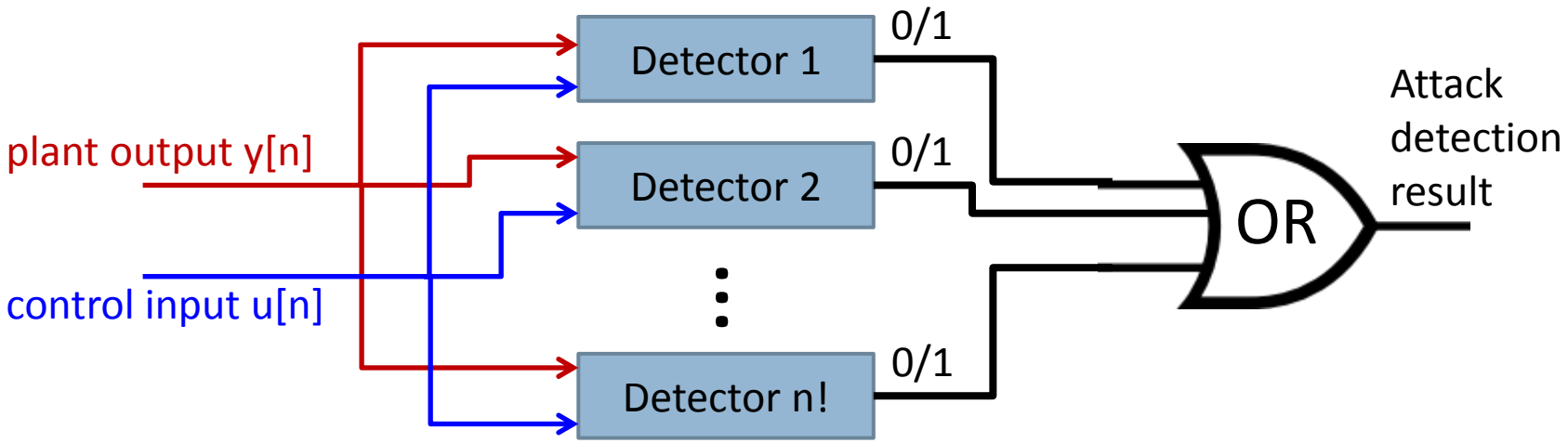
- Use fault detector to detect integrity attack
  - Attack behaves like natural faults
    e.g., surges, ramps, random noises
  - Effective under **Kerckhoffs's setting** (enemy knows everything)?



Applied to detect fault-like integrity attacks [HiCoNS'14]

Results

- Bypass by quadratic programming
- Non-bypassable **detector bank** for *n*-dimensional LTI system
  - Tampers with either control or sensor data only
  - General case: $O(n!)$
  - Converged system: $O(n)$



On Applying Fault Detectors against Fault Data Injection Attacks in Cyber-Physical Control Systems. D.Q. Vu, R. Tan, D.K.Y. Yau. INFOCOM 2016.

Observations

- Safety (maintain state in a safe region)
  - FDI
  - Attacker may optimize FDI based on learned model
- Stability (bounded input, bounded output)
  - Attack templates (delay, scaling)
  - Stability under attack vs. response speed to disturbance
- Fault detector != attack detector
  - Construct attack detector based on fault detectors

Acknowledgement

- ADSC & Illinois
  - Prof. Zbigniew Kalbarczyk
  - Prof. Ravishankar K. Iyer
  - Hoang Hai Nguyen
  - Dr. Xinshu Dong
- NTU
  - Prof. Hoay Beng Gooi
  - Dr. Eddy. Y. S. Foo
- SUTD
  - Prof. David K. Y. Yau
  - Quyen Dinh Vu