UCI University of California, Irvine

Hierarchal Decision Making in Smart Grid Under Cyber Security Attacks

Prof. Marco Levorato, Igor Burago, Peyman Tehrani

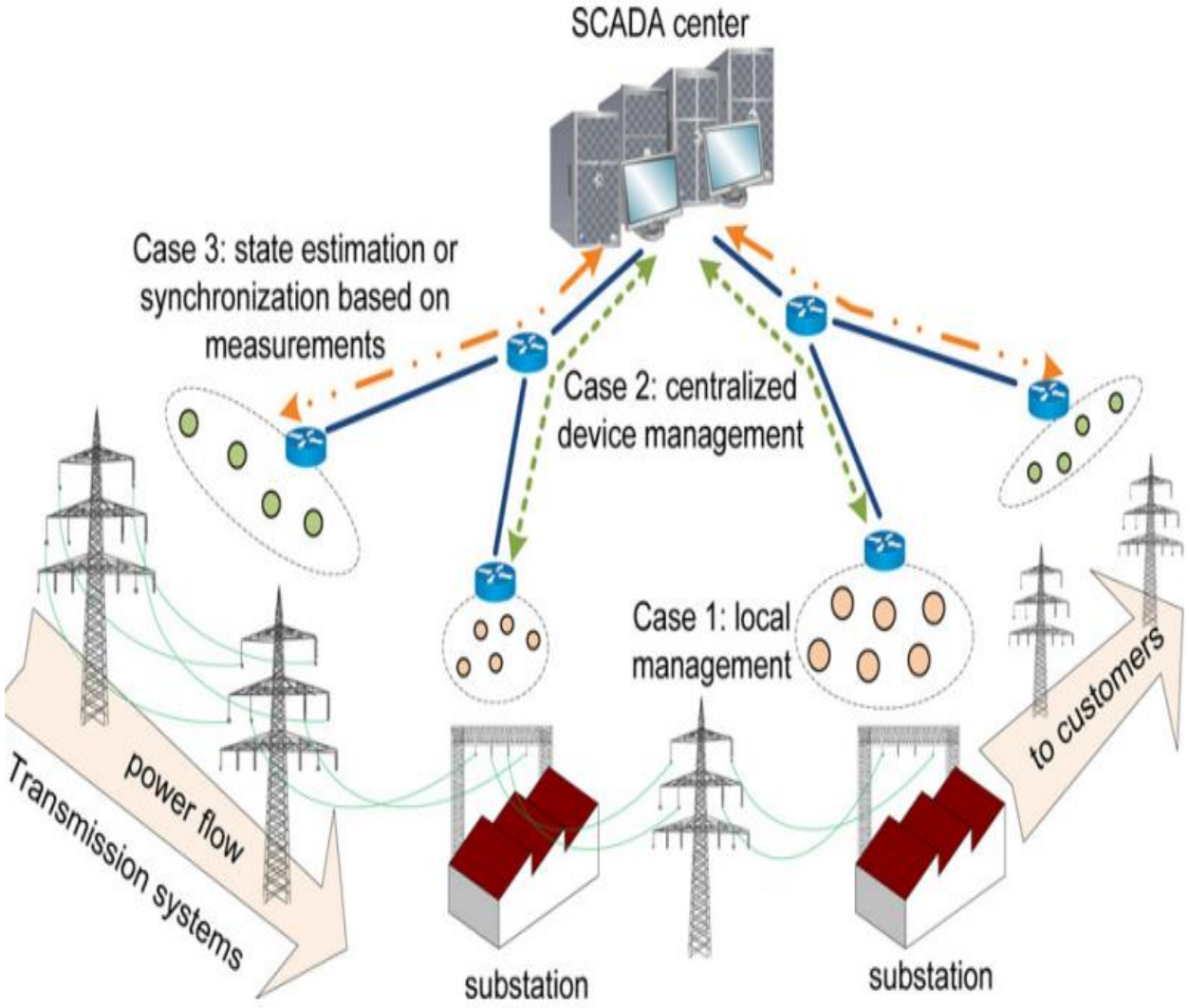
March 08, 2018

Overview

- Review of the cyber attacks in smart grid
- Need of more robust decision making mechanism in smart grid under cyber security attacks
- Proposing hierarchal classifiers and controllers
- Provide the proof of convergence of the proposed algorithm
- Simulation Results
- Conclusion

Smart Grid Architecture

- Local monitoring, control, and protection of power equipment's and devices in substations
- Centralized monitoring and control of power equipment's at the SCADA center
- State estimation based on measurements from raw data samples

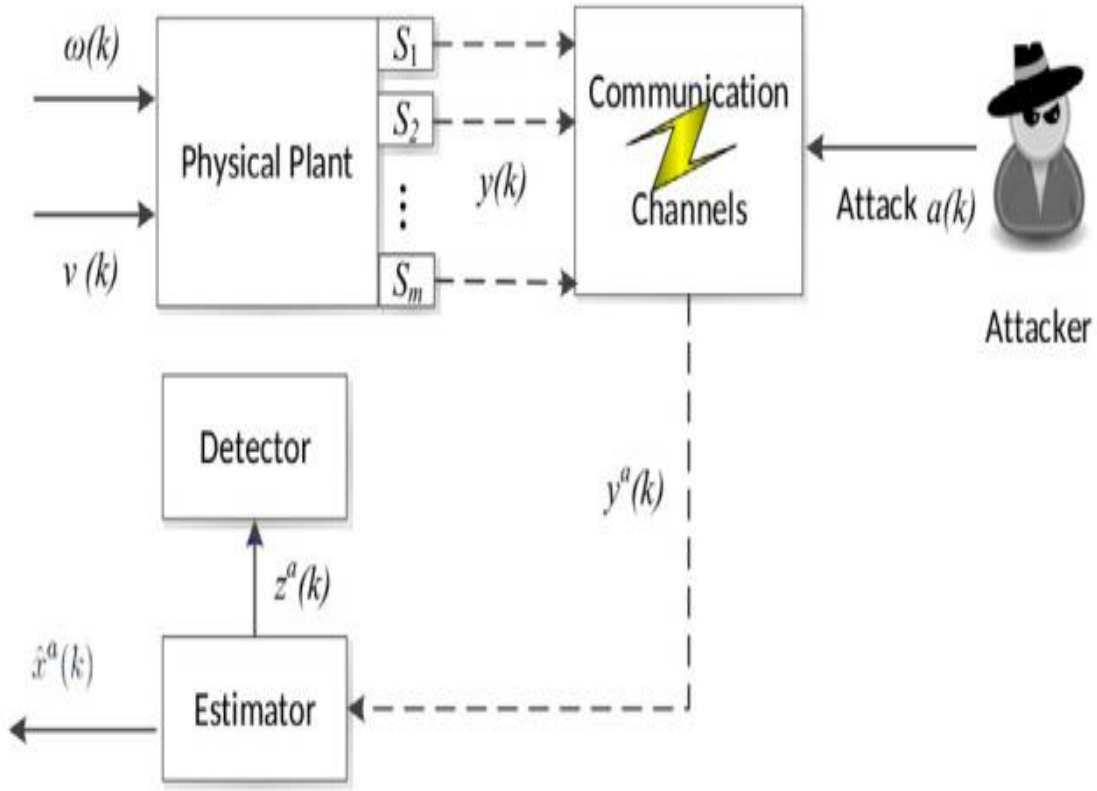


State Estimation under attack

- False data injection (FDI) :
  Add malicious fake data to meter measurements

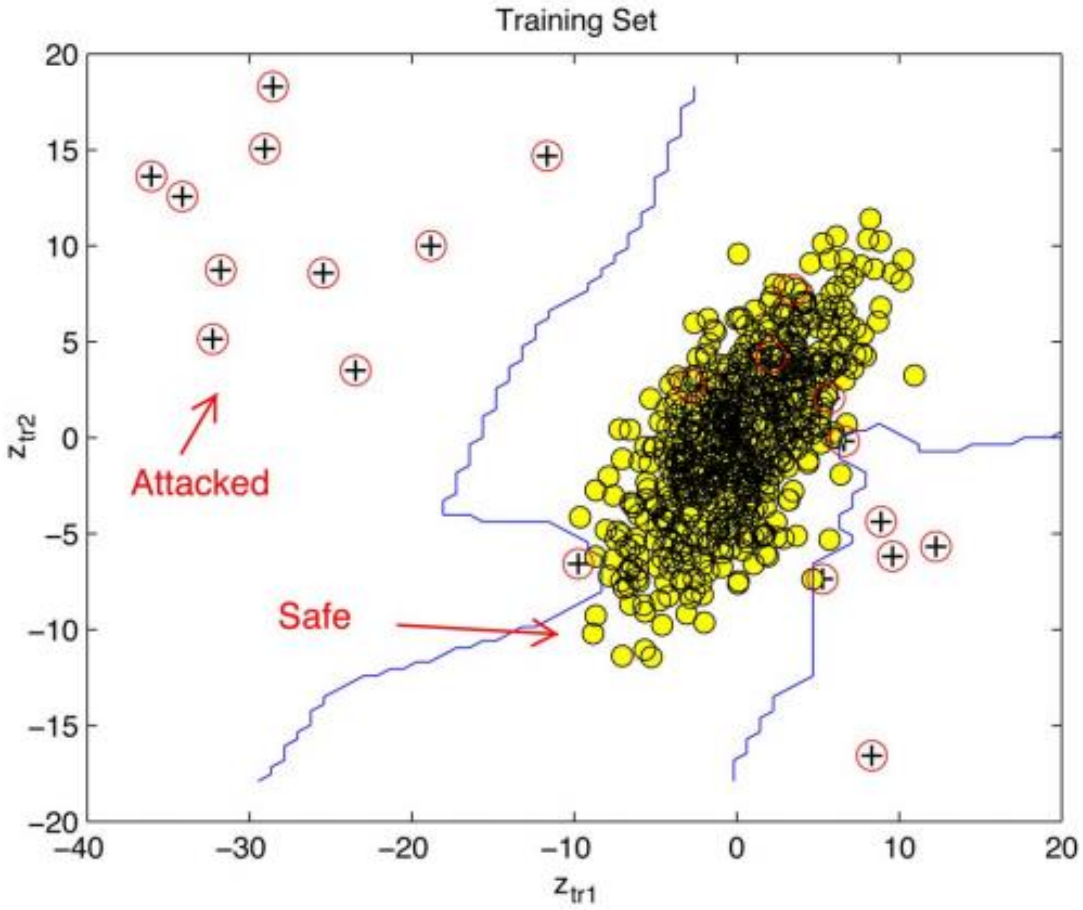
- Denial of service (DoS):
  Block the access of system to meter measurements

- Jamming:
  Corrupting the communication channel between the sensors (PMUs) and the controller



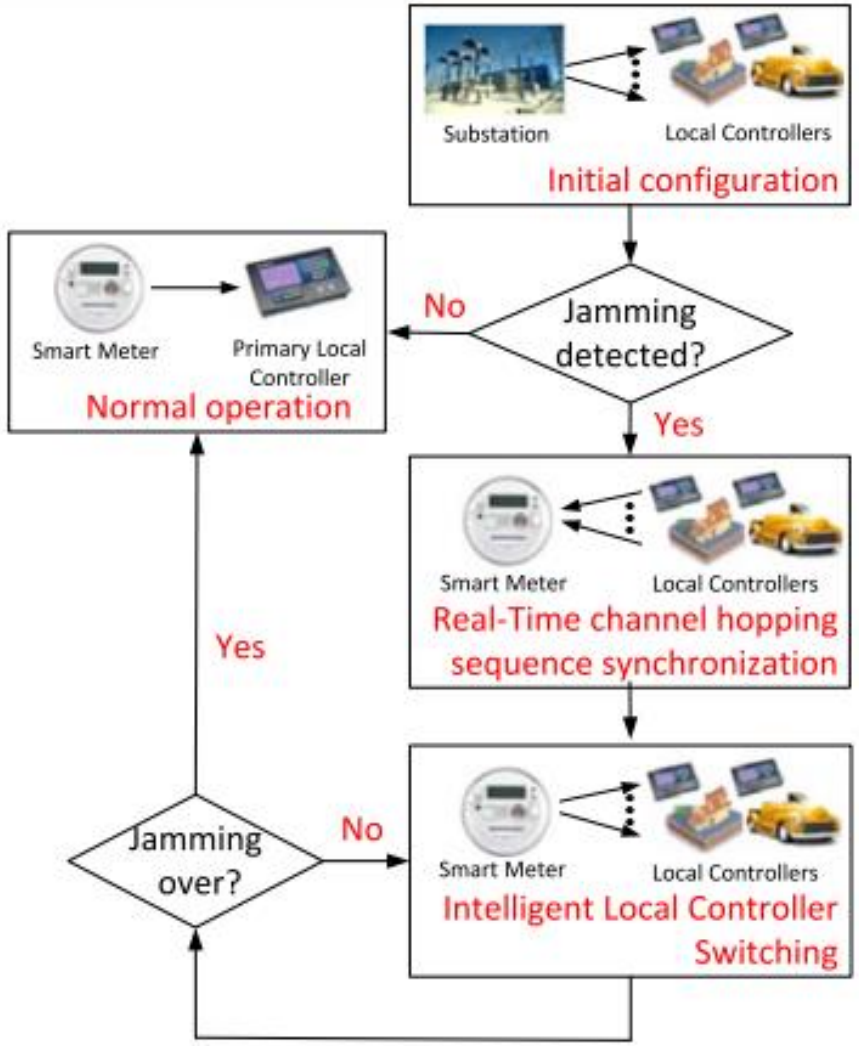
Machine learning for FDI detection

- Using complex nonlinear classifiers
- Needs a lot of training samples
- Inference and decision making done in the Central controller
- Need times to train and high delay to react to attacks
- Training is offline and not robust to high dynamic distribution



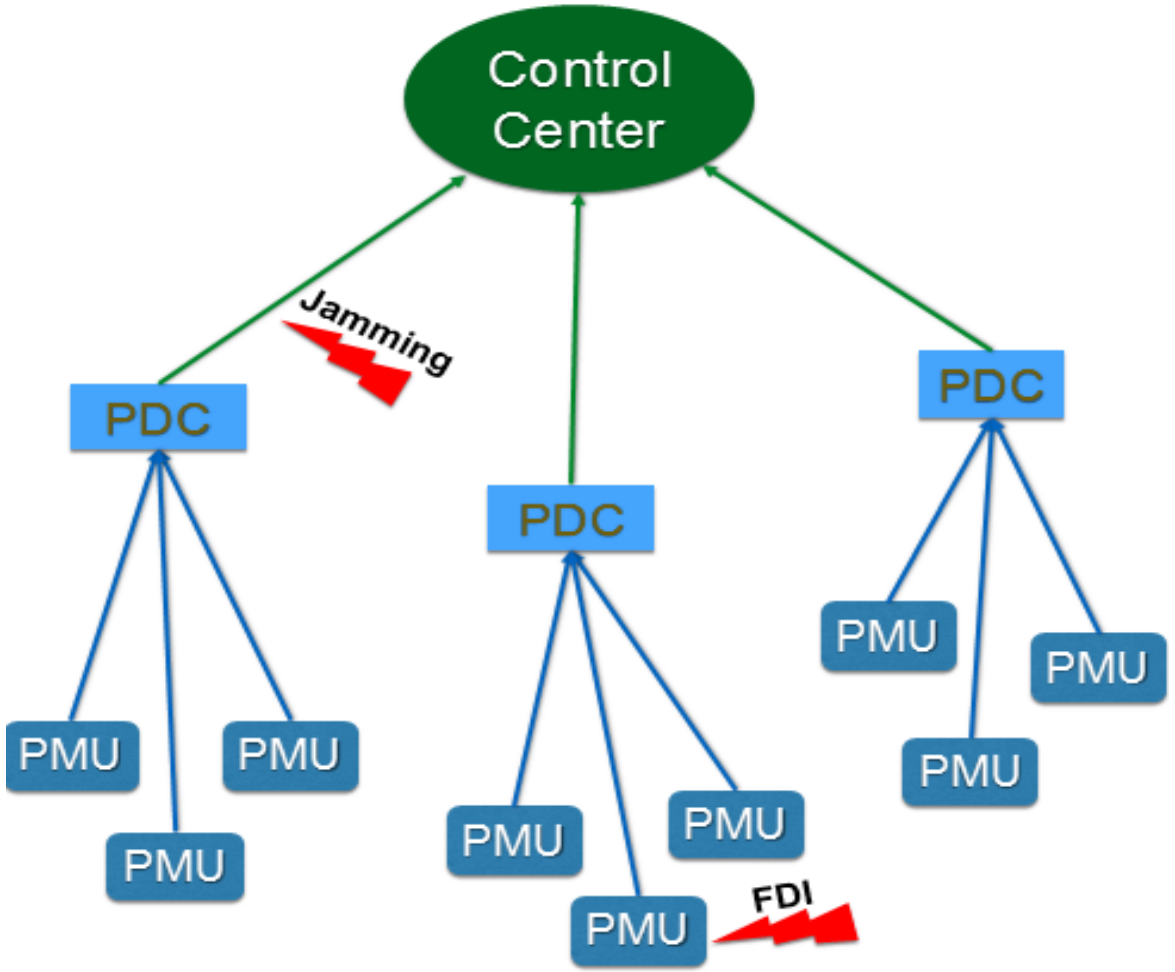
Approaches Against Jamming

- Most of the studies rely on channel hopping techniques
- Limited number of independent channels between the meters and the local controllers in larger networks
- limited channel resources available on each local controller make the channel hopping technique insufficient



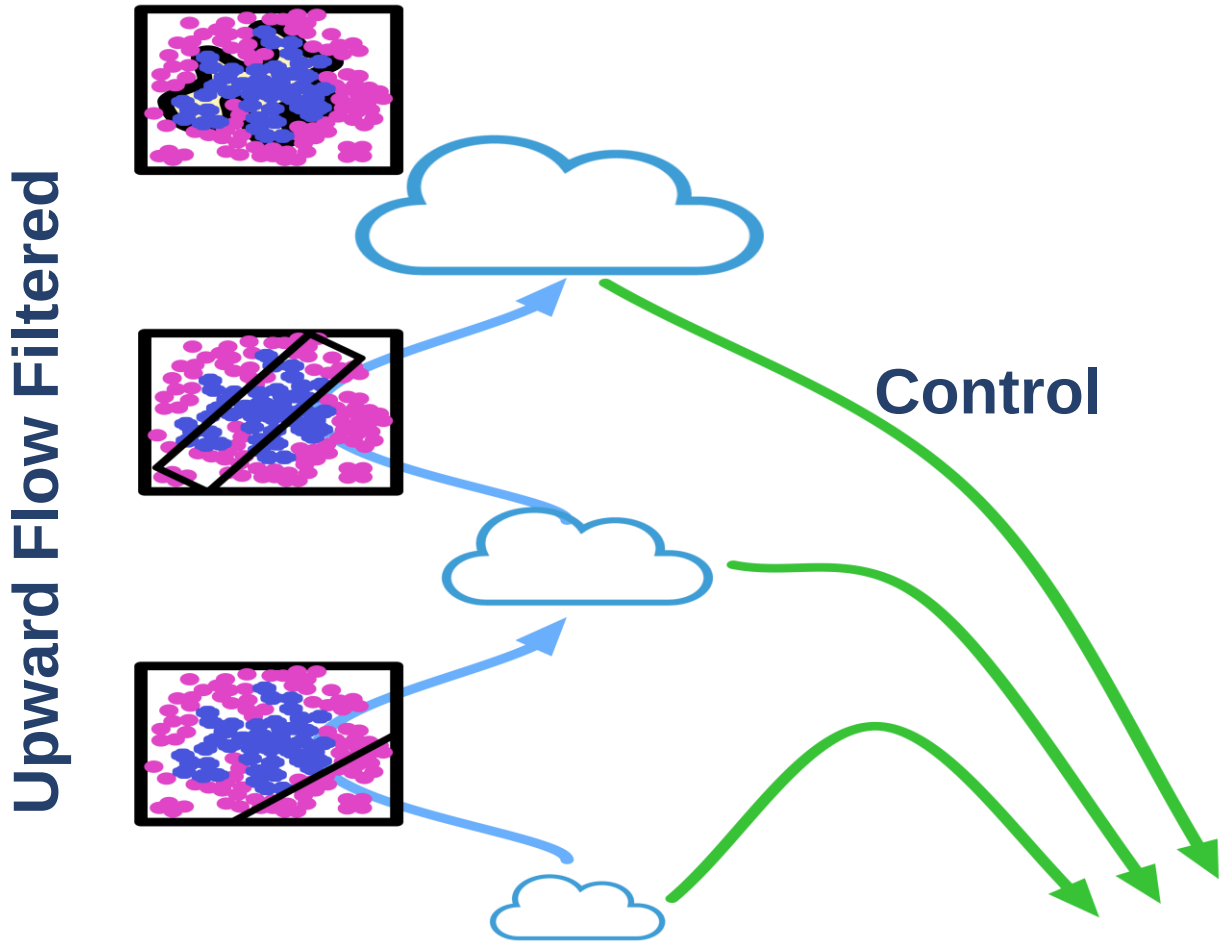
Need more resource efficient and robust method

- hierarchical architecture is more robust due to its redundant nature
- Analyzes the data close to real-time
- Prioritize the traffic flow from the lower to higher layer for the anomalies
- Use the available channels for only reporting anomalies/unsafe data in a limited resource scenario

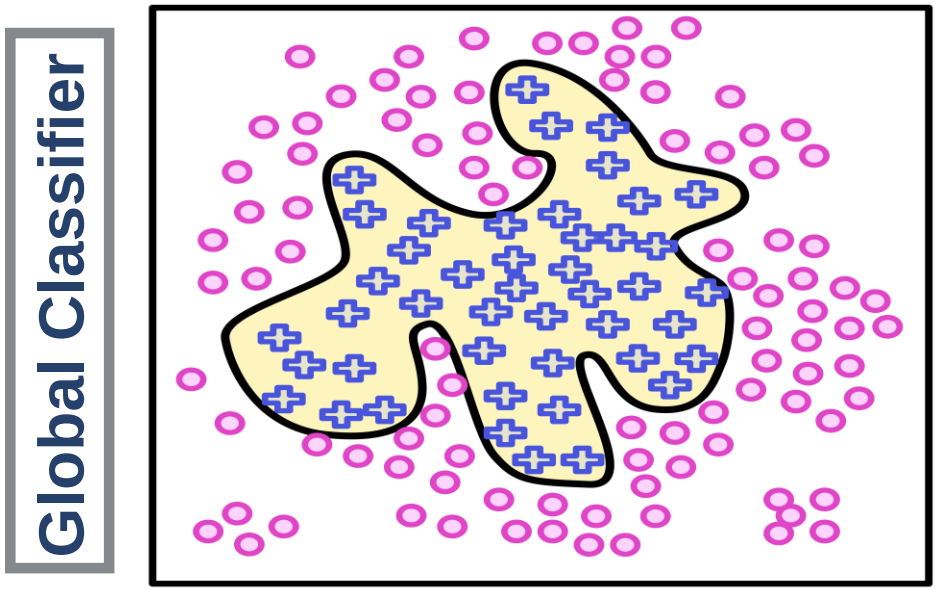


Network of Classifiers/Controllers

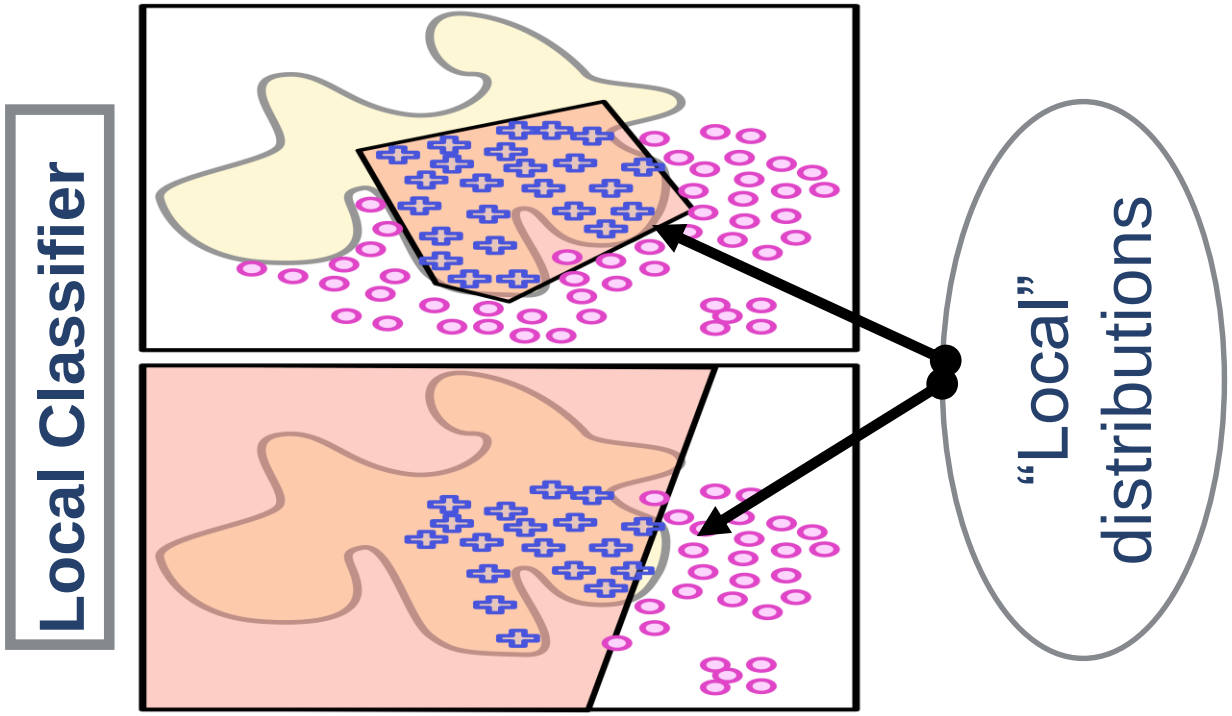
- Pipeline of Classifiers
- Sequence of classifiers of decreasing complexity
- Reduced bandwidth (reduced risk of congestion, more resilient to attacks)
- Fast control and low delay decision making



Global vs Local Classifiers



- Complex separating surface obtained through a very complex classifier
- Using all features
- Trained to achieve high accuracy in any context



- Context-induced distributions of samples may lead to context-specific good classifiers
- Training on the fly

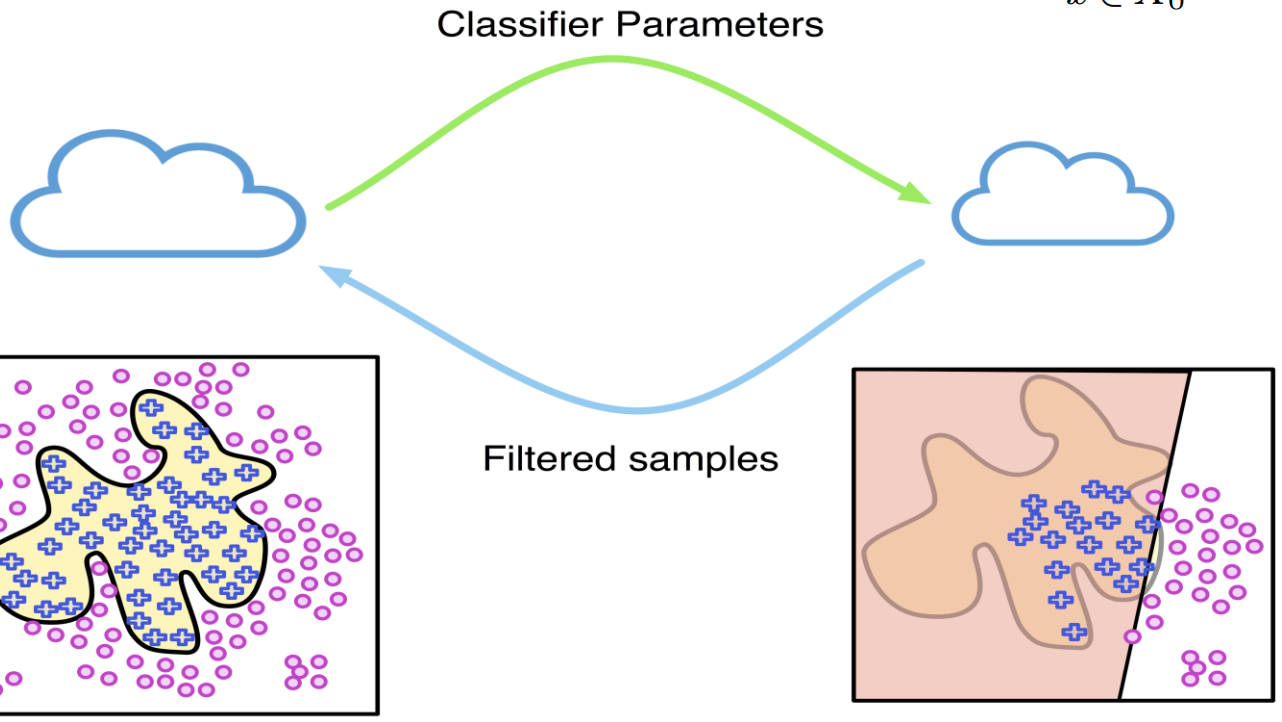
Preliminary Results: Online Classifier Training

Central Decision rule

$$\delta : Z \mapsto \{0, 1\}$$

Node Decision rule

$$f(x, \theta) \underset{x \in \widehat{X}_0}{\overset{x \in \widehat{X}_1}{\gtrless}} \mu$$



- Stochastic Optimization Algorithm
- Proof of convergence

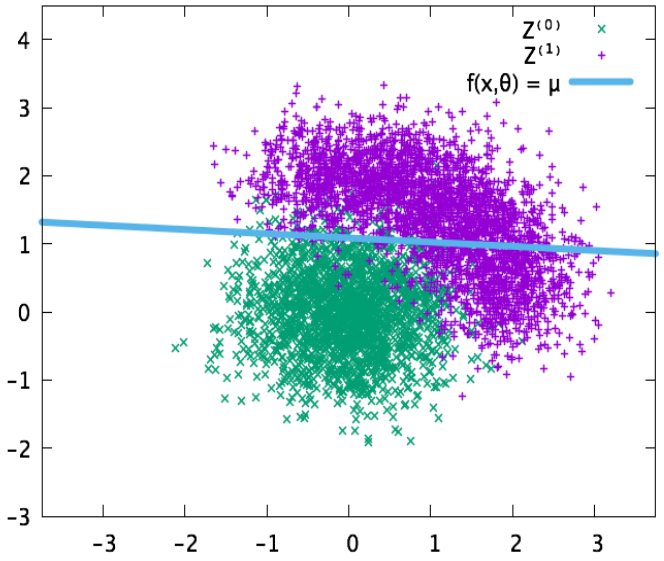
$$\tilde{\theta}_{t+1} = \theta_t - \gamma_t J(z_{t+1}, \theta_t, \mu_t) \nabla_\theta f(x_{t+1}, \theta_t)$$

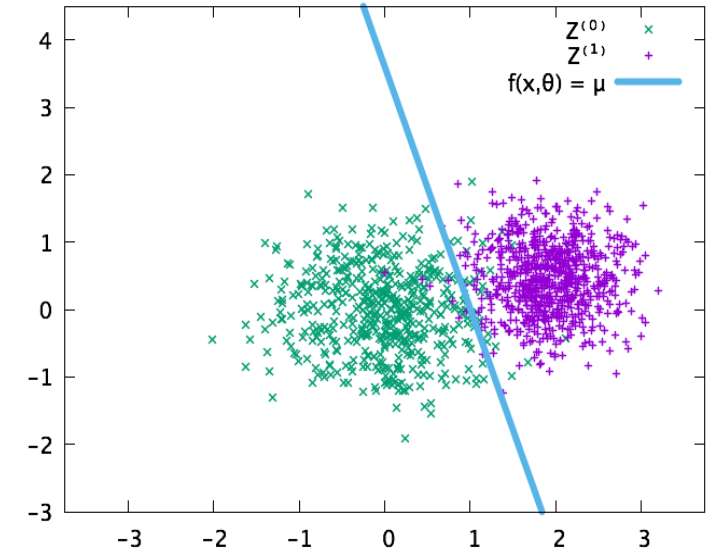
$$\tilde{\mu}_{t+1} = \mu_t + \gamma_t J(z_{t+1}, \theta_t, \mu_t),$$

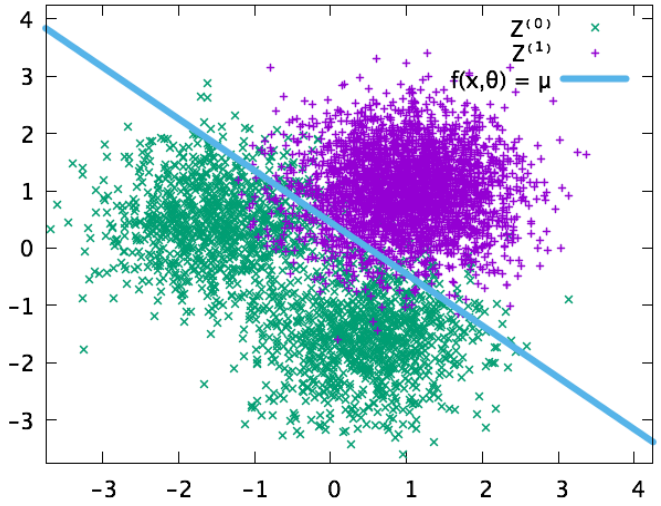
$$\mathrm{vec}(\theta_{t+1}, \mu_{t+1}) = \mathcal{H}_D\big(\mathrm{vec}(\tilde{\theta}_{t+1}, \tilde{\mu}_{t+1})\big)$$

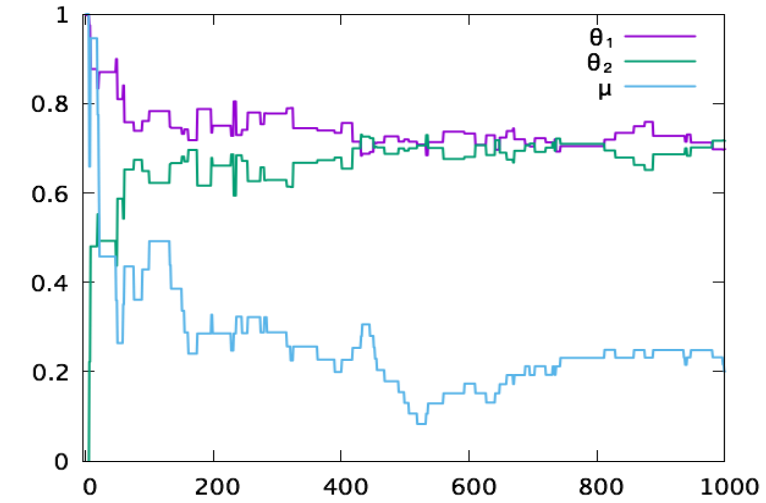
$$J(z, \theta, \mu) \triangleq \hat{I}_\mu^{(1)}\big(f(\chi(z), \theta)\big) - I_1(z)$$

Simulation Results









Conclusion

- Proposed hierarchal classifiers/ controllers
- Using low complexity classifier as getting closer to meters devices
- Achieving low delay decision making mechanism
- Global classifier in the central controller updates the parameters of lower level classifiers
- Derived the proof of convergence

Published Papers

- I.Burago and M. Levorato, “Randomized Edge-Assisted On-Sensor Information Selection for Bandwidth-Constrained Systems”, Published in Fifty-second Asilomar Conference on Signals, Systems and Computers, Asilomar, CA, Oct. 28-30, 2018.

- I.Burago and M. Levorato, “Cloud-Assisted On-Sensor Observation Classification for Constrained Decision-Making in Latency-Impeded IoT Systems”, Submitted to IEEE ISIT 2019, July 7-12 2019, Paris, France.