Secure Information Fusion For Cyber-physical Systems

Motivation

Cyber-Physical Systems (CPS) are integrations of computation, networking, and **physical** processes.

Attacks on CPS

- Confidentiality attack
- Availability attack
- Integrity attack

Examples

- Stuxnet
- Ukraine' power plant hack
- GPS spoofing
- ICS-CERT reported 295 cyber incidents for industrial control systems in 2015 in U.S.

Project Description

Project Goal

- Efficiency: Lower the cost of security
- Resilience: Provide performance guarantees

System Model

- Linear time invariant (LTI) system with multiple sensor monitoring

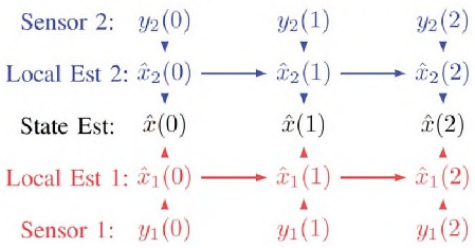
$$x(k+1) = Ax(k) + w(k),$$
$$y_\iota(k) = C_\iota x(k) + v_\iota(k), \text{ for } \iota = 1, \ldots, m$$

Attack Model

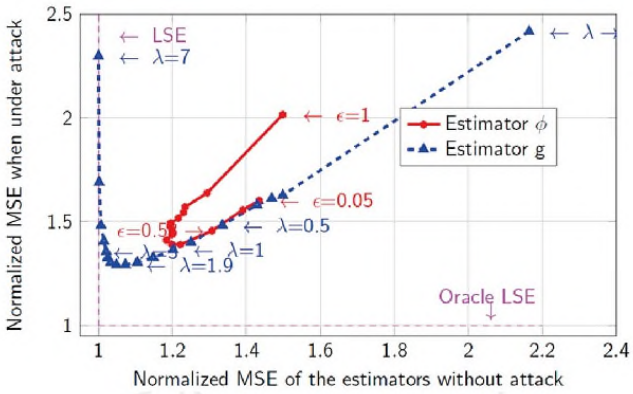
- At most p out of m sensors are compromised
- The attacked measurement can be arbitrarily changed

Main Result

- Need to fuse historical data from heterogeneous sensors together



- Each sensor perform an optimal local information fusion to generate a local state estimate
- The global estimate is then computed via convex programming from the local estimates
- Merits:
  - Security guarantees
  - Low computation complexity
  - Comparable performance to the MMSE estimator (which is not secure) when the CPS is not being attacked



Future Work

- CPS security is of utmost importance and is becoming real problem for the society
- Combine different security approaches to provide security in depth:
  - Hardware security
  - Software security
  - Communication security
  - System theoretic security
- We are planning to apply our techniques (alongside other security approaches) on an autonomous vehicle platform

Yilin Mo, Duo Han and Lihua Xie

School of Electrical & Electronic Engineering, Nanyang Technological University