Robust Hybrid Controller Design: Cyber Attack Mitigation Strategy for Cyber-Physical Systems

Cheolhyeon Kwon and Inseok Hwang

Research Background

- What is Cyber-Physical System(CPS)?

: CPSs consist of both logical elements such as embedded computers and physical elements connected by communication channels such as Internet.

- Existing Research Areas to Study the Security of CPSs

Information Security (Computer Science)	Secure Control (System Theory)
Focus on **data validation**; Integrity, Confidentiality, Authentication, Availability, etc.	Focus on a system's **dynamic-behavior**; Physical dynamics, Observer dynamics, etc.

- Research in Cyber Security from **Computer Science** Perspective

→ Key component of **hardware/software layer** in computer controlled system

→ **Do not address the dynamical behavior of the CPS under cyber attacks**

- Scope of this study: **Secure control theoretic perspective**

→ **Implement a secure control** with the ability of **adapting the system** with respect to **various cyber attacks**

➡ **Hybrid Control Scheme**

Problem Formulation

- System dynamics: Discrete-time deterministic linear time invariant system

$$x_a(k+1) = Ax_a(k) + Bu(k) + \boldsymbol{B_c a(k)}$$

State under cyber attack — Control input — Cyber attack

- Control Law: Linear state feedback control

State feedback gain matrix

$$u(k) = \boldsymbol{K(k)} x_a(k)$$

- Measure for Attack Effectiveness: Quadratic Performance Criteria

$$J(\boldsymbol{u}_{[\tau_1,\tau_2]}, \boldsymbol{a}_{[\tau_1,\tau_2]}) := \sum_{k=\tau_1}^{\tau_2-1} (x_a{}^T(k) Q_c x_a(k) + u^T(k) R_c u(k)) + x_a{}^T(\tau_2) Q_c x_a(\tau_2)$$

Evaluate the **cyber attack performance** during time interval $[\tau_1, \tau_2]$.

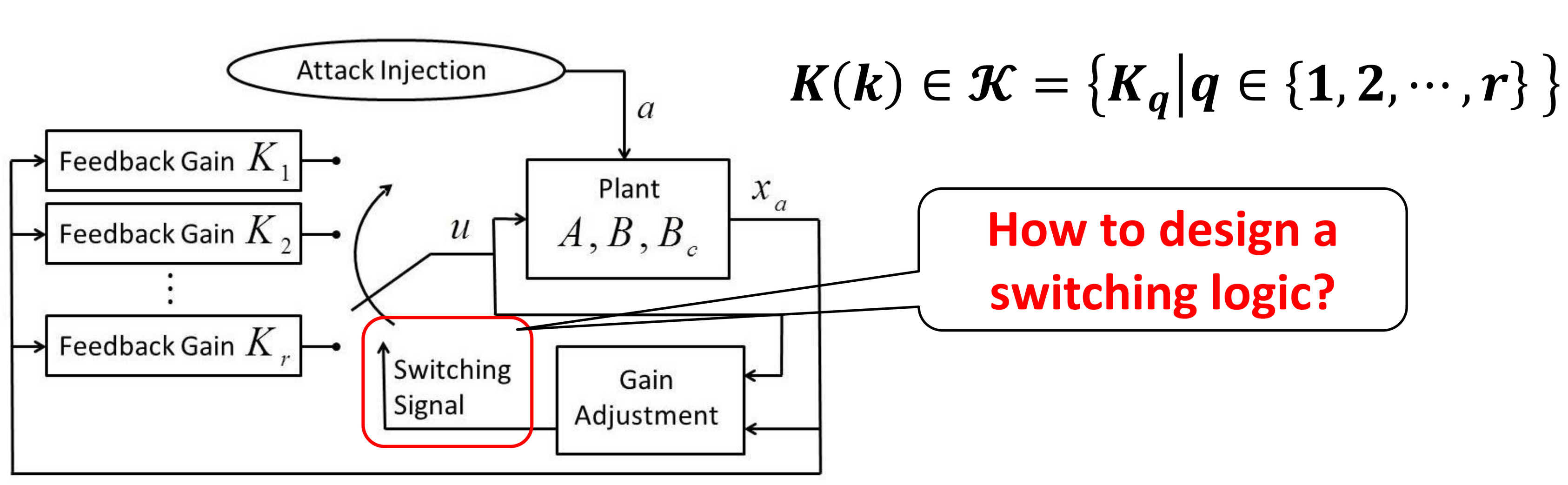
- **Cyber Attack Mitigation Problem**:

$$\min_{\{K(k),\forall k\in\{1,\cdots,N\}\}} J(\boldsymbol{u}_{[0,N]}, \boldsymbol{a}_{[0,N]})$$

Unknown *a priori*!

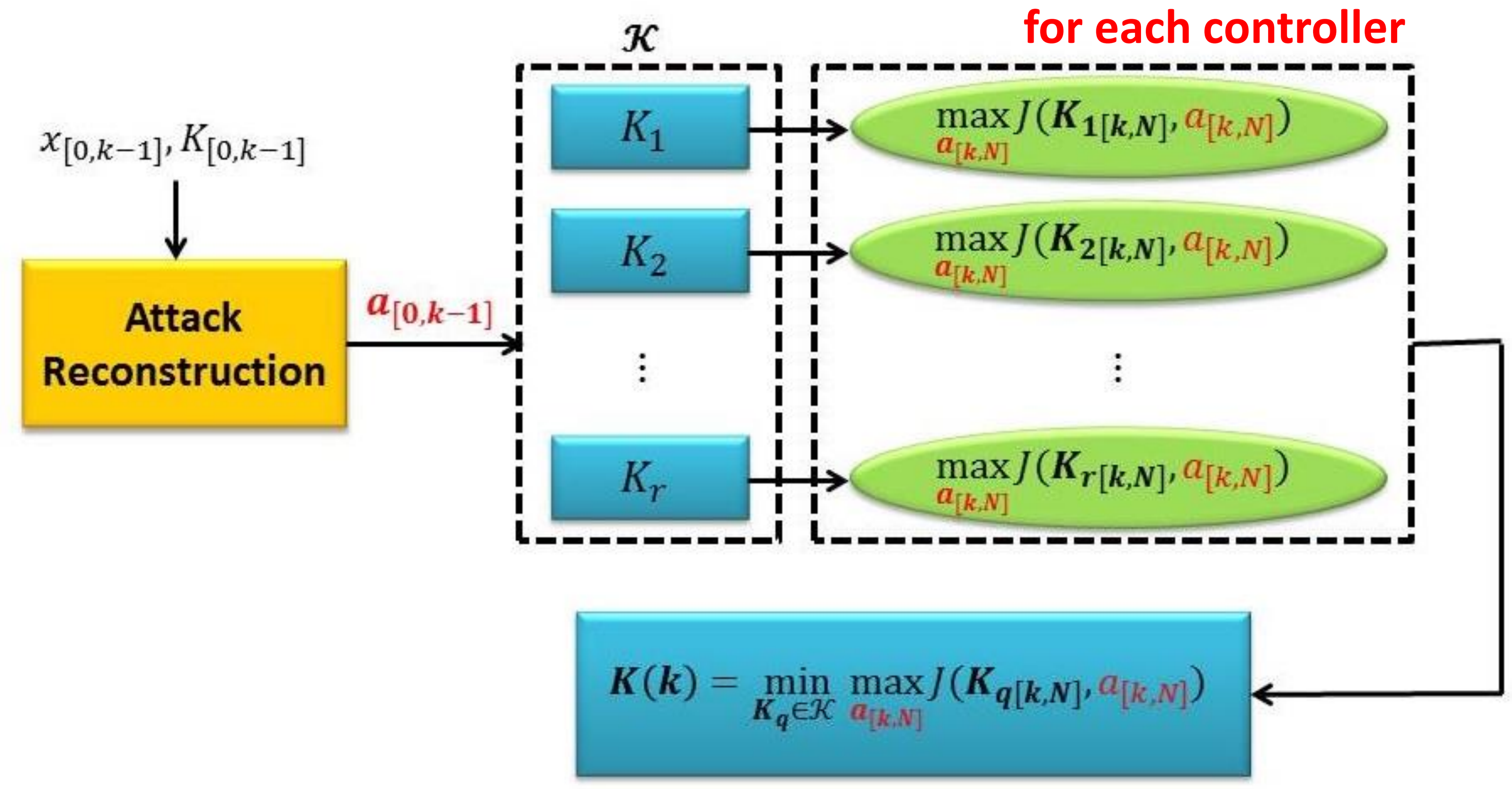
- **Hybrid controller** consists of **multiple sub-controllers**

$$\boldsymbol{K(k)} \in \boldsymbol{\mathcal{K}} = \{\boldsymbol{K_q} | \boldsymbol{q} \in \{\boldsymbol{1,2,\cdots,r}\}\}$$



Main Results

On-line Switching Algorithm for Robust Hybrid Control



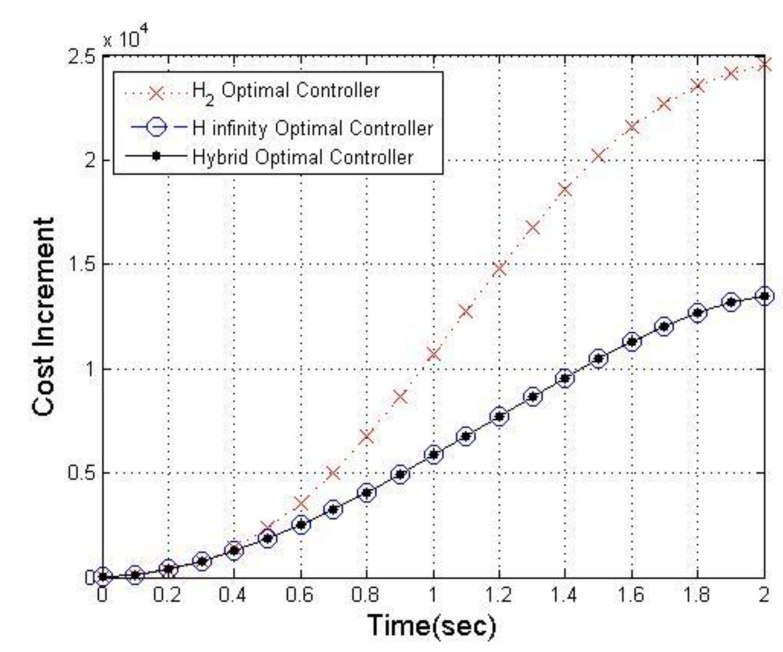
Illustrative Examples

- Special Class of **Hybrid Robust Controller** containing **Two Sub-Controllers → Hybrid H_2-H_∞ Controller**

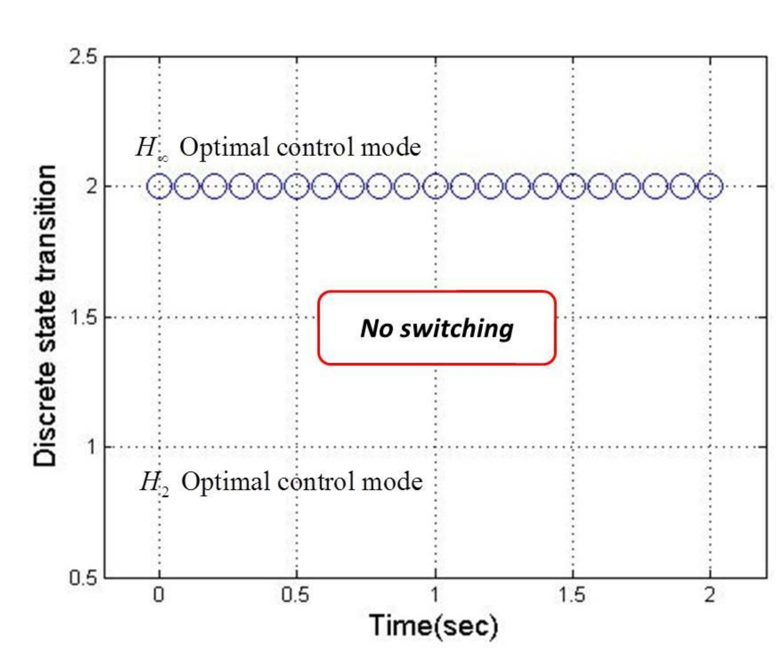
- **H_2 Optimal Controller**: optimized to counter a **random or noise attack**
- **H_∞ Optimal Controller:** optimized to counter a **worst-case attack**

- Applied CPS Example: **Rotorcraft Unmanned Aerial Systems (UASs)**
- Two types of cyber attacks are considered: the **worst-case attack** and **random attack**

- Simulation #1: **Worst-Case Attack Sequence**

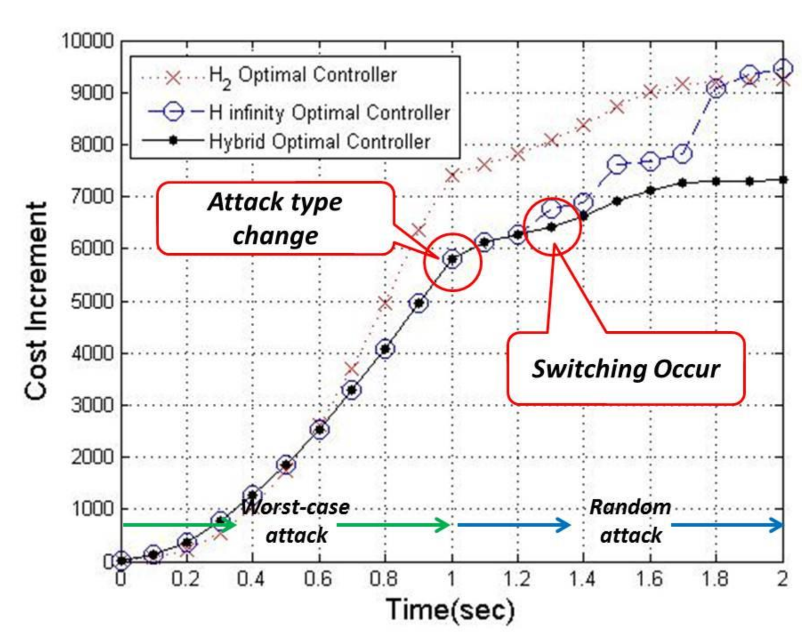


Cost increment

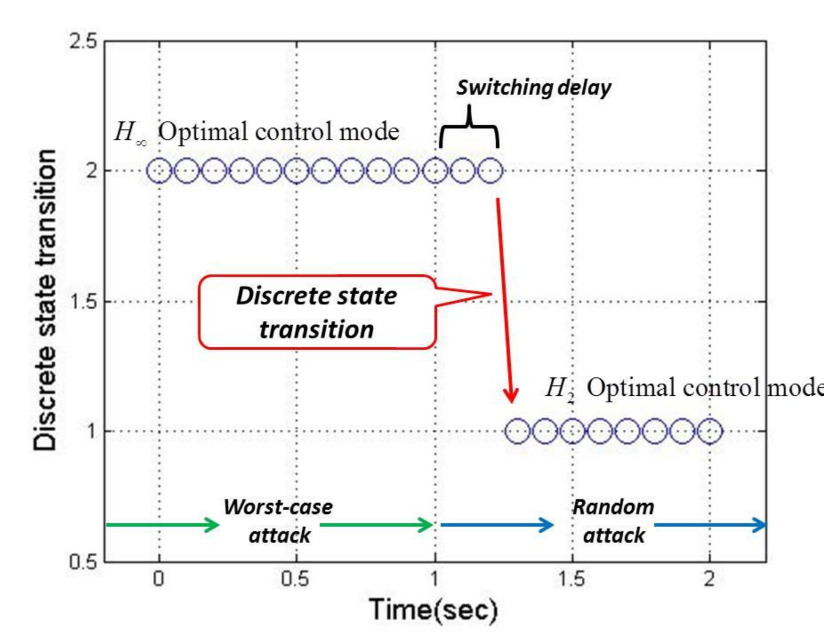


Switching history

- Simulation #2: **Worst-Case and Random Attack Combined Sequence**



Cost increment



Switching history