# CERIAS

The Center for Education and Research in Information Assurance and Security

# Security Analysis for Cyber-Physical Systems against Stealthy Cyber Attacks

Cheolhyeon Kwon and Inseok Hwang

## Motivation

- 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.

- Main research areas to analyze the security for CPSs.

| | Information Security (Computer Science) | Secure Control (Control Theory) |
|---|---|---|
| Function | Focus on data validation; Integrity, Confidentiality, Authentication | Focus on system's macro-behavior; Physical dynamics, Filter dynamics |
| Techniques | - Cryptography; Encryption / Decryption<br>- Firewalls<br>Signature based / Anomaly detection through white-list | - Robust and Resilient Control<br>- Fault-Tolerant Control; Fault Detection and Identification<br>- Distributed Estimation |
| Drawback | Do not address the dynamical behavior of the CPS during cyber attacks. | There is very little work accounting for faults caused by a vague adversary |

*- The safety tools only using information security are not sufficient for secure control of CPSs. In this work, we are focused on analyzing the system's response during cyber attacks from the control theoretic perspective.*

## Problem Formulation

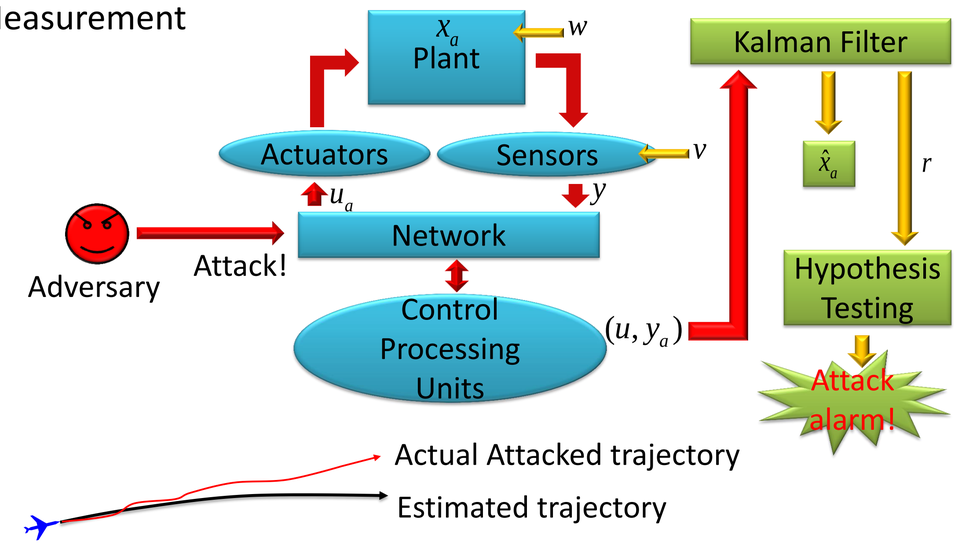
- System dynamics: Stochastic Linear Time Invariant model

$$x(k+1) = Ax(k) + Bu(k) + B_a^c u_a^c(k) + w(k)$$

System's state; Control input; Cyber attack; Gaussian noise

$$y(k) = Cx(k) + B_a^o u_a^o(k) + v(k)$$

Measurement




⟶ **<u>Stealthy cyber attack:</u> cause large estimation error without being detected by the monitoring system.**

⟶ *Under which conditions the attacker has a capability to exhibit such dangerous stealthy cyber attacks?*

## Main Results

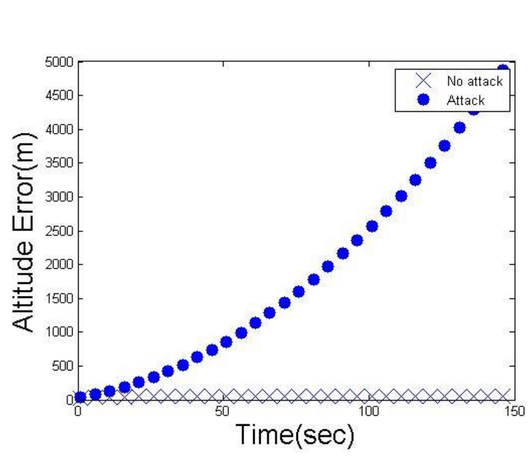
**<u>Stealthy Cyber Attack Classification</u>**

| Attack Case | Compromised Component | Possible Effect |
|---|---|---|
| Case 1 | Actuators only | Injected attack sequences can cause only the limited estimation error to avoid being detected. |
| Case 2 | Sensors only | Attack sequences gradually falsify the data so that the residual power does not become large enough to trigger an attack alarm. Attackers can eventually induce the infinite estimation error as time goes to infinity, while not being detected. |
| Case 3 | Both sensors and actuators | Attackers can manipulate the estimation error insofar as attacked input is physically admissible. Moreover, since the resulting residuals are not changed in their statistical property, any residual based monitoring systems are of no use against this type of attacks. |

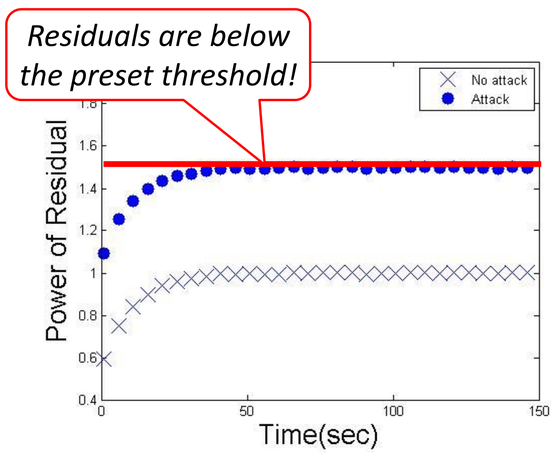
## Illustrative Examples

- Stealthy cyber attacks to state estimators in Air Traffic Control system (ATC): Attack case 2 (Sensor compromise only).

- Monte Carlo simulation of the worst stealthy cyber attack in $\alpha-\beta$ filter.



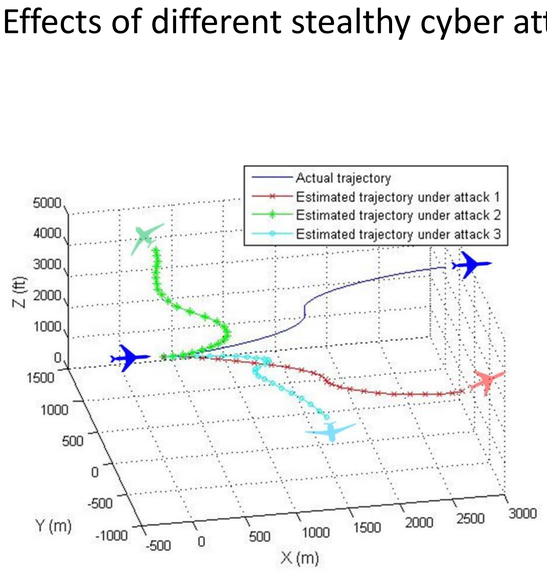

*<u>Altitude Estimation Error</u>*



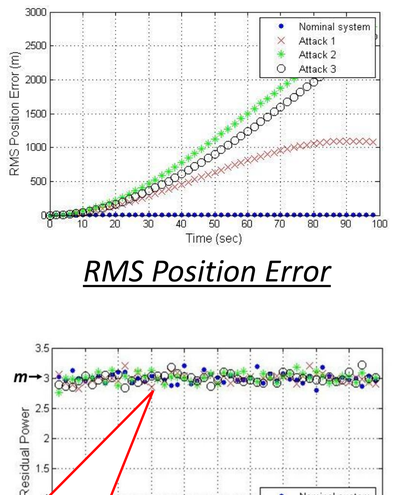

*<u>Hypothesis Test Statistics</u>*

- Stealthy cyber attacks to Unmanned Aerial Vehicle (UAV) Navigation System: Attack case 3 (Both sensor and actuator compromise).

- Effects of different stealthy cyber attacks on the 3-D tracking of the UAV.




*<u>Trajectory Estimates</u>*




*<u>RMS Position Error</u>*




*<u>Test Statistics</u>*