Security Analysis for Process Control Systems

Zong-Syun Lin†, Alvaro A. Cárdenas‡, Saurabh Amin‡, Hsin-Yi Tsai†,
Yu-Lun Huang† and Shankar Sastry‡

† National Chiao Tung University, Taiwan
‡ University of California, Berkeley

ABSTRACT

We present security analysis of process control systems (PCS) when an attacker can compromise sensor measurements that are critical for maintaining the operational goals. We also develop model-based detection methods that can be tuned to limit the false-alarm rates while detecting a large class of sensor attacks. By taking example of a well studied process control system, we discuss the consequences of sensor attacks on the performance of the system and important implications for designing defense actions.

1. ATTACK MODEL

A general model for the observed signal is the following:

$$\tilde{y}_i(k) = \begin{cases} y_i(k) & \text{for } k \notin \mathcal{K}_a \\ y_i(k) + \lambda_i(k) & \text{for } k \in \mathcal{K}_a \\ y_i^{\min} & \text{for } k \in \mathcal{K}_a,\ y_i(k) + \lambda_i(k) < y_i^{\min} \\ y_i^{\max} & \text{for } t \in \mathcal{K}_a,\ y_i(k) + \lambda_i(k) > y_i^{\max} \end{cases}$$

The model can be used to represent many attacks such as additive injection, multiplicative scaling, replay & DoS.

2. MODEL-BASED ATTACK DETECTION

The anomaly detection module (ADM) of our attack detection system (Figure 1) compares the sequence $\tilde{y}(k)$ (received from the sensor and may have been attacked) with the sequence $\hat{y}(k)$ (obtained from the internal model). The ADM raises an alert if the deviation between the two sequences is significant. The nonparametric CUSUM statistic for sensor i is $S_i(k) = (S_i(k-1) + z_i(k))^+$, $S_i(0) = 0$.

Our response strategy (shown in Fig 1) can be summarized as follows: For sensor i, if $S_i(k) > \tau_i$ (the threshold selected for sensor i), the ADM replaces $\tilde{y}_i(k)$ with $\hat{y}_i(k)$. Otherwise, it treats $\tilde{y}_i(k)$ as the correct sensor signal. We use the Tennessee-Eastman process control system (TE-PCS) model (Figure 2) to verify our approach.

3. EXPERIMENTS

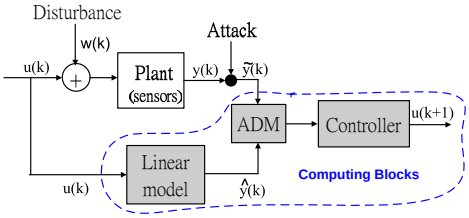


Figure 1: The proposed detection module.

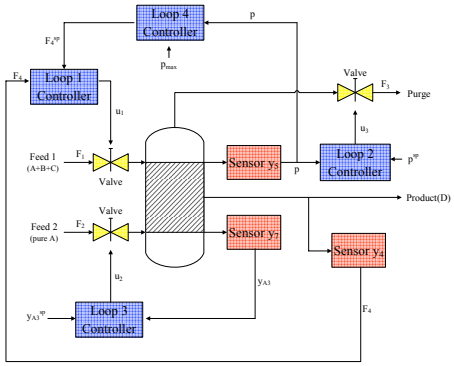
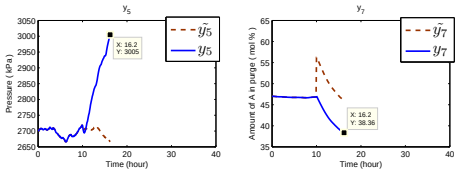
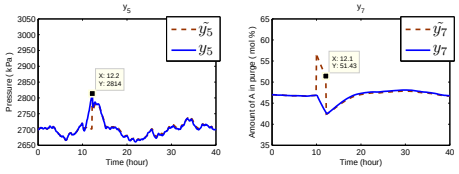


Figure 2: Architecture of the Simplified TE Plant



(a) without ADM the pressure grows past safety levels.



(b) The statistics for y_5 and y_7 independently detect the attack.

Figure 3: $\tilde{y_5}(t) = y_5(t-10)$ **&** $\tilde{y_7} = y_7 * 1.2$