A Study of a Cyber Threat Detection for Controller Process Signals Using an Extended Kalman Filter-based State Estimator

Jae Hwan KIM, Kwang Seop SON, Jae Gu SONG, Yong Gu LEE, Young Jun LEE
Security R&D Team, Korea Atomic Energy Research Institute
jhkim85@kaeri.re.kr

***Keywords : Cyber Threat Detection, Extended Kalman Filter (EKF), Process Signal Tampering**

1. Introduction

Cybersecurity threats targeting industrial control systems (ICS) pose serious risks to the safety and continuous operation of critical national infrastructure, such as nuclear power plants. In particular, if an attacker manipulates process control signals within the control system, it can lead to unintended abnormal operations, potentially resulting in unplanned shutdowns of the power plant as well as physical, economic, and social damages. Despite these risks, current cybersecurity frameworks for nuclear power plants have functional limitations, and an effective threat detection system tailored to control systems has yet to be developed. Therefore, this study proposes a state estimation method based on the Extended Kalman Filter (EKF) to detect signal tampering in process input signals of industrial control systems.

2. Control systems of NPPs

The control systems of domestic nuclear power plants are classified as non-safety grade and include key control systems such as the Feedwater Control System (FWCS), Steam Bypass Control System (SBCS), Reactor Regulating System (RRS), Pressurizer Level Control System (PLCS), and Pressurizer Pressure Control System (PPCS) [1]. These control systems perform automatic process control functions to maintain the normal operation of the reactor and Balance of Plant (BOP) systems, playing a crucial role in ensuring the stable operation of the power plant. However, if the process variables of the control system are maliciously manipulated through a cyber-attack, the normal operating conditions may be disrupted, potentially leading to equipment malfunctions, unexpected reactor shutdowns (Scram), or severe transient conditions in the power plant.

3. Cyber threats targeting process variables

Process variables in industrial control systems (ICS) are essential for maintaining the safety and continuous operation of nuclear power plants. Cyber threats targeting these variables can disrupt normal operations or distort operator situational awareness by employing signal tampering techniques. In particular, attacks that manipulate the input signals (process signals) of control systems alter sensor data, causing the control system to perceive a state different from reality. This can lead to the execution of incorrect control commands or a compromise in system safety.

To detect such process signal tampering attacks, an effective approach is to predict the normal signal range based on a physical model of the controlled plant and compare it with actual sensor measurements. This study proposes applying a state estimator using the EKF to detect tampering in process signals. Since nuclear power plant process signals exhibit complex dynamic behavior, a highly reliable detection method that accounts for sensor noise and measurement uncertainty is required. EKF operates effectively in such environments and enables early detection of anomalies in sensor data, allowing for the rapid identification of process signal tampering attacks. This study proposes a detection method utilizing an EKF-based state estimator and evaluates its feasibility by applying it to a simplified plant model to assess its effectiveness in detecting cyber threats.

4. Process signal state estimation and cyber threat detection in control systems

4.1. Extended Kalman filter

The Extended Kalman Filter (EKF) is a state estimation technique for nonlinear systems, designed as an extension of the Kalman Filter (KF) to accommodate nonlinear dynamics [2]. In industrial control systems (ICS), dynamic systems are typically represented by differential equations, which can be converted into discrete-time domain equations describing the relationship between state variables over time.

For example, in a linear system, the state equation can be expressed as:

$$(1)\ \dot{x} = Ax(t)$$

When discretized, it takes the form:

$$(2)\ x(k+1) = x(k) + Ax(k)\Delta t$$

Based on these state equations, the Extended Kalman Filter predicts the current system state, compares it with measured sensor values, and computes an optimal state estimate. If there is a discrepancy between the plant model's predicted values and the sensor measurements,

the Kalman Gain is adjusted to minimize this difference, ensuring a more reliable state estimation. While the conventional Kalman Filter assumes linear system dynamics, the Extended Kalman Filter is adapted for nonlinear systems by locally linearizing the system using a Taylor series expansion before applying the Kalman filter algorithm.

The core principle of the Extended Kalman Filter is as follows: it estimates the optimal system state by comparing the predicted state variables with sensor measurements. If the plant model has high noise, the filter assigns more weight to sensor measurements, whereas if sensor measurements are noisy, the model's predicted values are given more weight. This adaptive weighting is automatically determined through the Kalman Gain, enabling effective detection of process signal tampering.

4.2. System modeling and simulation

EKF estimates system states using sensor output values and a system model while removing measurement noise to provide reliable state information [3]. To achieve this, the EKF compares the estimated state with the predicted state based on the system model, analyzing the difference between the two values to detect anomalies. The core concept of cyber threat detection using a state estimator is residual analysis. The residual is defined as the difference between the estimated value and the predicted value, which can be expressed as follows:

$$(3)\ r_k = \hat{y}_k(EV) - \hat{x}_k(PV)$$

Here, $\hat{y}_k$ represents the estimated value obtained using the Kalman Filter, where measurement noise is removed, while $\hat{x}_k$ is the predicted value calculated solely based on the plant model's input values. Under normal operating conditions, these two values remain similar. However, when process signal tampering or a cyber-attack occurs, the difference between them increases. By analyzing this residual, it is possible to detect abnormal operations in the system. The state estimation process of the KF consists of the following five steps: (1) Initialization: The initial state vector x_0 and the initial covariance matrix P_0 are set. (2) Prediction of the estimated value and covariance: The next state is predicted based on the system model.

$$(4)\ \hat{x}_k = A\hat{x}_{k-1}$$

$$(5)\ P_k = AP_{k-1}A^T + Q$$

Here, A represents the state transition matrix, and Q is the process noise covariance matrix. (3) Kalman Gain Calculation: The Kalman Gain is computed to combine the predicted state with the sensor measurement.

$$(6)\ K_k = P_k H^T (HP_k H^T + R)^{-1}$$

Here, H represents the measurement matrix, and R is the measurement noise covariance matrix. (4) Estimation Update: The state is updated using the Kalman Gain.

$$(7)\ \hat{x}_k = \hat{x}_{\bar{k}} + K_k(z_k - H\hat{x}_{\bar{k}})$$

Here, z_k represents the sensor measurement. (5) Error Covariance Update: The covariance matrix is updated.

$$(8)\ P_k = P_{\bar{k}} - K_k H P_{\bar{k}}$$

In this study, the CUSUM (Cumulative Sum) algorithm is utilized to enhance the accuracy of detecting sensor signal tampering.

To verify the effectiveness of the proposed EKF-based anomaly detection method, a simplified water tank system was modeled and simulated. The water tank dynamics follow a nonlinear differential equation based on the tank geometry and fluid flow assumptions:

$$(9)\ A\frac{dH}{dt} = bV - a\sqrt{H}$$

where H is the water level in the tank, A is the tank cross-sectional area, and V is the control input voltage. The inflow is proportional to the input voltage, while the outflow depends on the square root of the water height. b is the inflow coefficient, representing how the voltage V affects the water inflow rate. a is the outflow coefficient, related to the rate of discharge through the outlet based on the water height.

To validate the proposed EKF-based anomaly detection method, a simulation testbed was constructed using a simplified water tank system model, as shown in Fig. 1. The testbed includes a PID-controlled plant model, a level sensor with noise, and the proposed EKF-based detection mechanism. A cyber-attack scenario was simulated by injecting a constant bias into the sensor signal path. This setup enabled a comparative analysis of detection behaviors under both normal and tampered conditions.

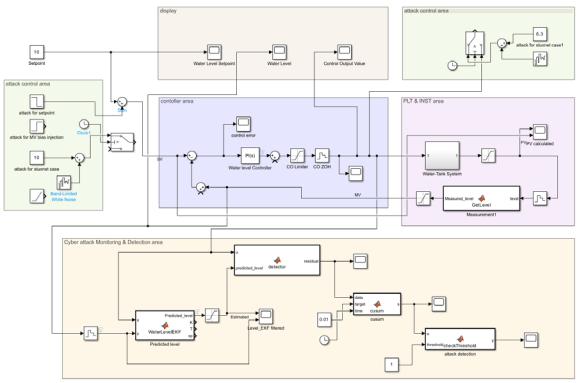

Fig. 1 Simulation model for EKF-based cyber threat detection in simplified water tank system

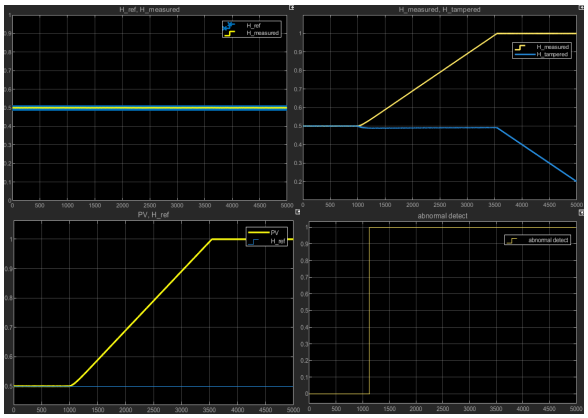

Fig. 2 EKF-based anomaly detection under sensor signal tampering attack in a water tank control system

A stealthy attack was simulated by gradually decreasing the measured water level signal while the actual tank level continued to rise. As shown in Fig. 2, the PID controller, misled by the manipulated signal, increased the inflow, resulting in tank flooding. The proposed EKF-based anomaly detector successfully identified the onset of the abnormal condition shortly after the attack initiation, demonstrating its effectiveness in detecting signal tampering attacks before physical damage occurred.

5. Conclusions

In this study, we proposed a method for detecting process signal tampering in control systems by applying an EKF-based state estimation approach. The proposed method compares sensor output values with predicted values from the plant model, analyzes the residual (difference between the two values), and utilizes this analysis to detect cyber threats. Through preliminary experiments, we confirmed that applying the EKF-based state estimator effectively detects cyber-attacks, such as process signal tampering.

REFERENCES

[1] Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co., Ltd., "APR1400 Design Control Document Tier 2, Chapter 7: Instrumentation and Controls," APR1400-K-X-FS-14002-NP, Rev. 3, Aug. 2018.
[2] S. J. Julier and J. K. Uhlmann, "New extension of the Kalman filter to nonlinear systems," Signal Processing, Sensor Fusion, and Target Recognition VI, vol. 3068, SPIE, 1997.
[3] S. F. Schmidt, "Application of state-space methods to navigation problems," in Advances in Control Systems, vol. 3, Elsevier, pp. 293-340, 1966.