CYBER-PHYSICAL SECURITY IN MODERN WATER TREATMENT FACILITIES

Overview

Modern water treatment facilities are critical infrastructure systems that rely on interconnected Industrial Control Systems, composed of sensors and actuators distributed across multiple treatment stages. These components continuously monitor physical and chemical parameters, and execute precise control actions to ensure a safe, stable, and uninterrupted water supply.

The Cyber Threat Landscape

With the rapid digitization of these systems and their integration with networking technologies for remote monitoring, automation, and centralized data analytics, their exposure to cyber threats has significantly increased. This creates more entry points that attackers can target. Hackers may interfere with communication networks, send false sensor data, alter control commands, or modify system settings, all while keeping the plant running in a normal manner.

Traditional monitoring systems that rely on fixed rules or simple thresholds often struggle to detect these subtle or well-planned attacks, especially when they closely resemble normal operational changes. Therefore, more intelligent and adaptive detection methods are needed to identify unusual patterns and protect the system effectively.

Problem Statement

Therefore, the problem can be summarized as detecting anomalies and cyber-attacks in real-time from multivariate time-series data generated by heterogeneous sensors across interdependent process stages, while maintaining high system availability and minimizing false alarms.

Key Difficulties Include:

- High dimensionality because of sensors with different scales and sampling rates.
- Complex inter-stage dependencies and cascading effects.
- Distinguishing between normal operational variations and malicious behavior.
- Strict real-time constraints (sub-second detection latency).
- High reliability requirements.

Objective

The objective is to design a system that maximizes attack detection capability (high recall) while maintaining acceptable precision to avoid unnecessary shutdowns, under real-time operational constraints.