Attack Detection System in Smart City Water Treatment Plants

Author: Dweep Hiten Vira (242240018)
Supervisor: Dr. S.S Udmale
Department: Computer Engineering & Information Technology, VJTI
Date: 2025-2026

Introduction

1. **The Vulnerability of Critical Infrastructure:** Modern society relies on critical infrastructure like power grids, transportation, and water treatment plants. These systems are managed by Industrial Control Systems (ICS) and SCADA, which bridge the physical and digital worlds. The increasing connection of these systems to IT networks, while improving efficiency, has also created a large cyber-attack surface.

2. **Beyond Data Theft:** Unlike traditional IT attacks that focus on stealing data, cyber-attacks on ICS can have severe, real-world consequences. For water treatment plants, this could mean an attacker manipulating chemical dosing, causing equipment damage, or even contaminating the public water supply. The stakes are incredibly high, as these attacks can directly impact public health and safety.

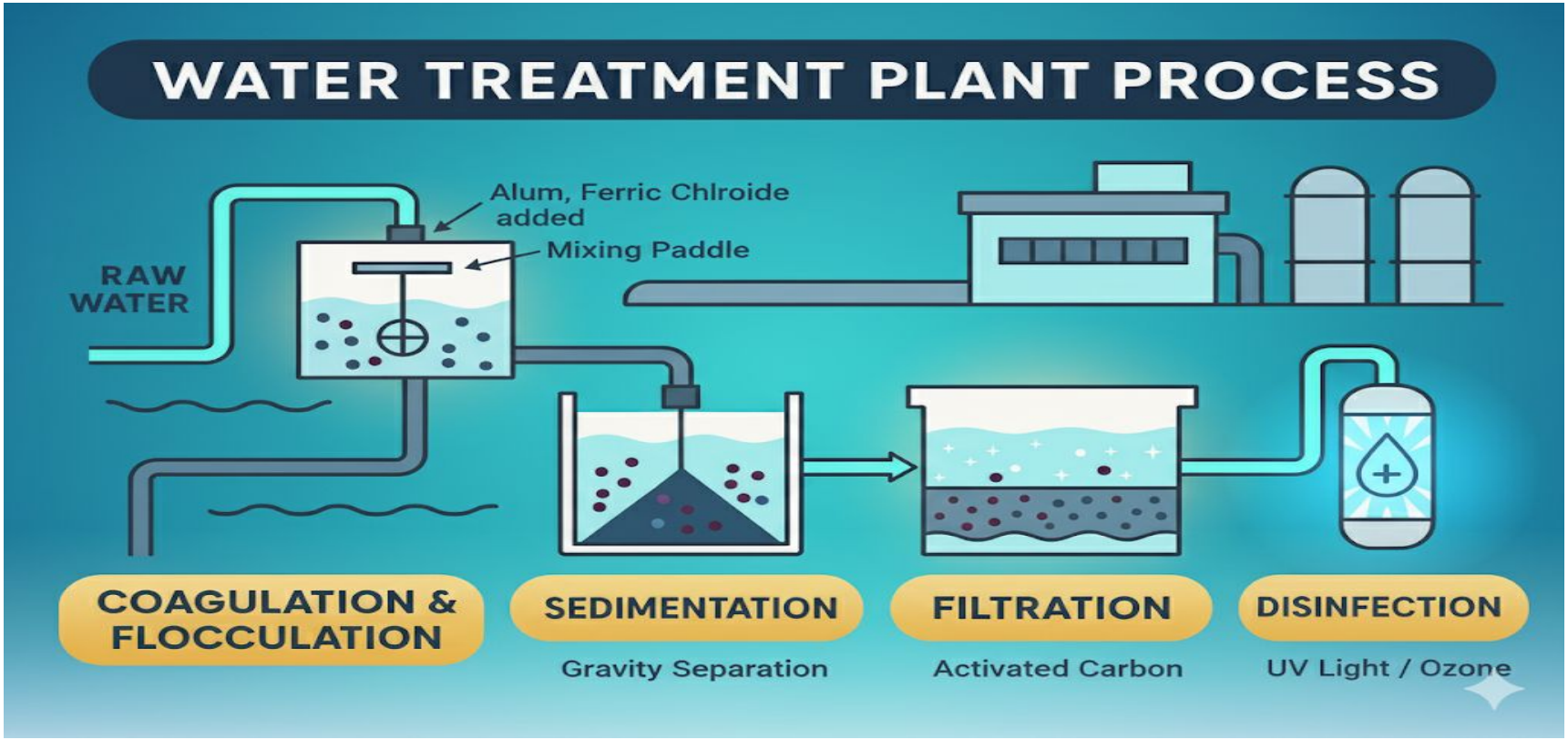
3. **The Fundamental Problem:** Developing an effective defense against these attacks is challenging due to the scarcity of realistic, high-fidelity datasets. You cannot experiment on a live water treatment plant. Existing datasets often lack the complexity and context of real-world cyber-physical interactions, making them unsuitable for training advanced machine learning models.

4. **Our Solution:** This research is motivated by the urgent need to address this data gap. Our solution is to build a high-fidelity SCADA simulator. This simulator will function as a safe and controlled environment to not only emulate the complex behaviors of a water treatment plant but also to generate a novel, labeled dataset that includes a wide range of sophisticated, real-world cyber-physical attack scenarios. This dataset will then be used as the foundation for developing and validating new intrusion detection systems.

Aim & Objectives

1. **Primary Aim:**
    a. Design and implement a high-fidelity SCADA simulator for a water treatment plant.
    b. Generate a comprehensive, labeled dataset for training and evaluating advanced intrusion detection systems.
2. **Specific Objectives:**
    a. Construct a modular simulator modeling cyber-physical interactions.
    b. Develop a framework for injecting context-aware cyber-physical attacks (False Data Injection, Malicious Command Injection).
    c. Generate a time-series dataset logging synchronized physical and cyber-level data.
    d. Systematically review relevant literature to inform the design.

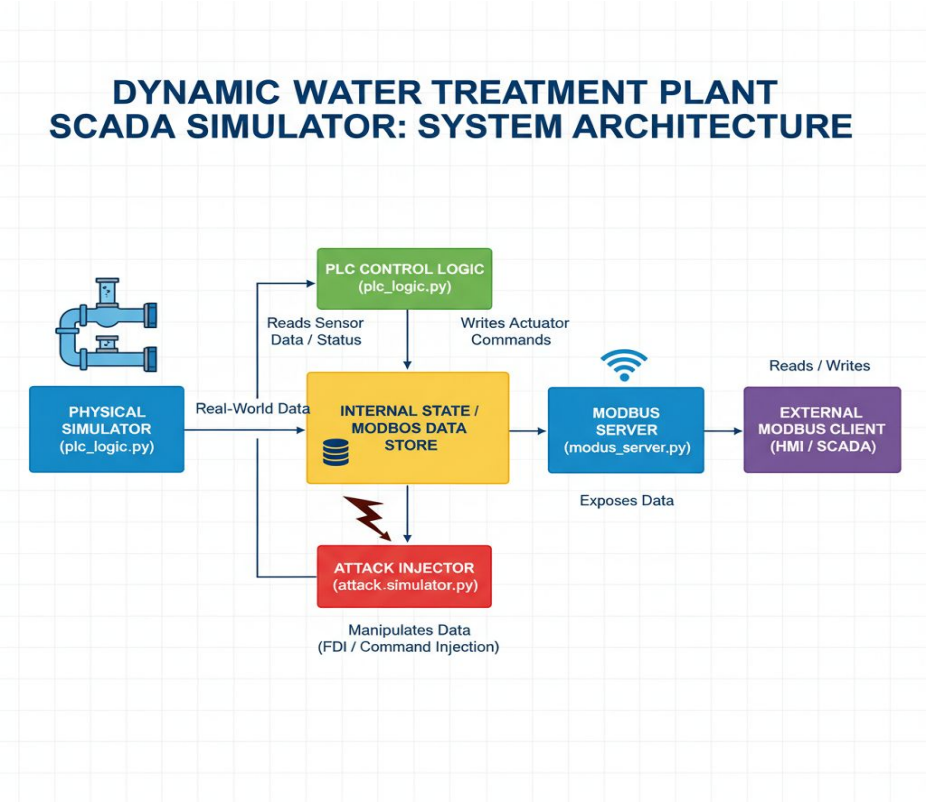
Water Treatment Plant Process Overview



Methodology - System Architecture

Key Components:

1. Physical Simulator: Models the real-world physics and "ground truth" of the plant.
2. Internal State: An in-memory database representing the cyber data (Modbus registers). This is the attacker's target.
3. PLC Control Logic: Emulates a PLC, reading sensor data and writing actuator commands.
4. Modbus Server: Exposes the data store to external clients (like an HMI).
5. Attack Injector: A privileged component for executing programmed cyber-physical attacks.



Attack Simulation & Data Generation

A 1-hour simulation run generated a labeled dataset with 51,000+ time-stamped data points.

Attack Scenarios:

1. Malicious Command Injection: An attacker directly manipulates actuator commands (e.g., setting a pump speed to 0).
2. False Data Injection (FDI): An attacker alters sensor readings to deceive the PLC (e.g., reporting false turbidity levels).
3. Stealthy Data Manipulation: A "low-and-slow" attack designed to evade simple threshold-based alarms.

Example of Attack Impact

CYBER ATTACK IMPACT ALALYSIS: EFORE & AFTER VALUES

Dynamic Water Treatment Plant SCADA Simulator

1. MALICIOUS COMMAND INJECTION (Orange)

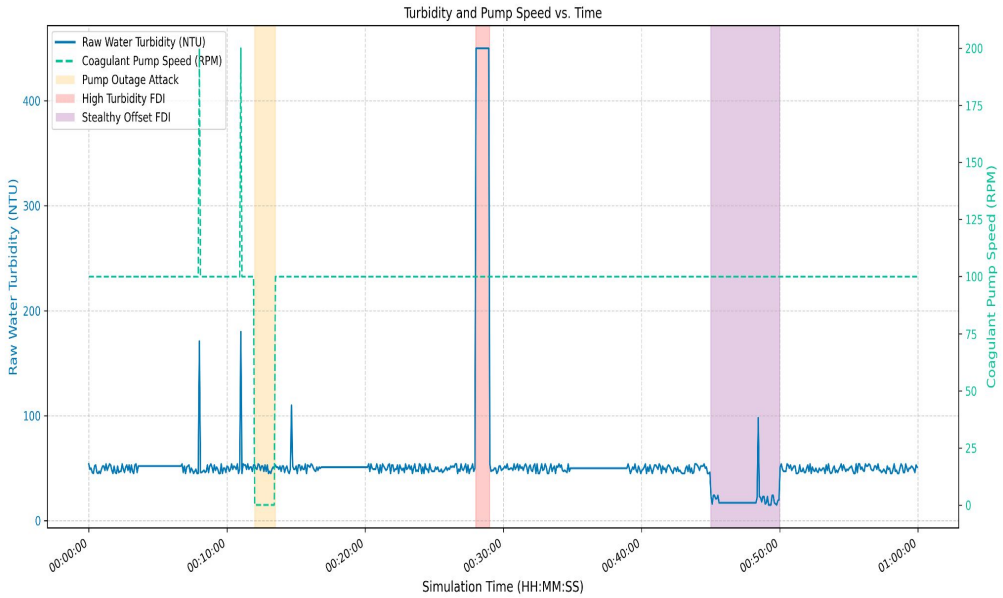
SIMULATION TIME			
00:11:59		METRIC A (Before Attack)	ACTIVE ATTACK
00:12:59	Pump Speed (Logic)	Actual: 100 RPM	None
	Pump Speed (Logic)	Pump Speed: 50 ↑	Short Coagulant Pump Outage
	Actual (Actual: 100 RPM	0 RPM ↓	

2. FALSE DATA INJECTION (Red)

SIMULATION TIME			
00:27:00		METRIC B Turbidity: Attack)	ACTIVE ATTACK
00:28:00	Actual Turbidity: 50 NTU	Reported 450 NTU ↑	None
	Reported 50 NTU	Brief False High Turbidity	200 ↑
	Pump Speed): 200 RPM	Brief False High Turbidity	

3. STEATHY DATA MANIPULATION (Purple)

SIMULATION TIME			
00:14:59		METRIC A (Before Attack)	ACTIVE ATTACK
00:45:00	Actual Turbidity: 55 NTU	Reported 55 NTU	Stealthy Turbidity Offset
	Actual Turbidity 200 RPM	Reported 25 NTU ↓	↓
	Pctual Turbidity: 90 RPM	Stealthy Turbidity Offset	



Conclusion and Proposed Work

1. We have successfully completed Phase 1 by developing a high-fidelity SCADA simulator and generating a comprehensive, labeled dataset. This addresses the critical need for realistic data in ICS cybersecurity research.
2. The modular framework and novel dataset are significant contributions, providing a solid foundation for future empirical research.
3. **Proposed Work (Phase 2):**
    a. Visualization and Data Understanding: The initial step will involve thoroughly visualizing the collected data. This includes understanding the ranges of normal values for all sensors and actuators, as well as the specific characteristics of each attack type. This process is crucial for effective feature engineering and model development.
    b. Model Application: We will apply various machine learning (ML) and deep learning (DL) algorithms to predict and classify attack types. The focus will be on the LSTM and GRU models, which are expected to excel at identifying the temporal patterns of sophisticated attacks.

Thank You!!