사이버안보연구, 3집 1호 2026 여름, 221-260

수처리 플랜트 OT/ICS에서 침입탐지 데이터셋 생성을 위한 시뮬레이터 설계 및 구현

0301-221260

안석현 | 단국대학교 일반대학원 인공지능융합학과(제1저자)
조성제 | 단국대학교 소프트웨어학과(교신저자)

* 이 논문은, 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-학석사연계ICT핵심인재양성 지원을 받아 수행된 연구(IITP-2026-RS-2023-00259867)이며, 또한 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학ICT연구센터(ITRC)의 지원을 받아 수행된 연구 (IITP-2026-RS-2023-00259967)입니다.

논문접수일 2026년 5월 14일 | 논문심사일 2026년 6월 11일 | 게재확정일 2026년 6월 19일

논문 요약

본 논문은 수처리 플랜트 OT/ICS 환경에서 침입탐지 데이터셋 생성을 위한 사이버보안 실험용 시뮬레이터를 설계하고 구현 결과를 분석한다. 실제 산업 설비에서 공격 데이터를 수집하는 것은 공정 안정성, 비용, 운영 중단 위험으로 인해 제한되므로, 통제된 조건에서 정상 운전과 공격 상황을 반복 생성할 수 있는 실험환경이 필요하다. 이에 본 논문에서는 정상 운전과 공격 상황을 통제된 환경에서 반복 재현할 수 있는 실험용 시뮬레이터를 제안한다. 해당 시뮬레이터는 수처리 공정 모델, PLC/HMI 제어 로직, 공격자 노드, Modbus/TCP 통신 환경을 결합하여, 네트워크 트래픽, 공정 상태 로그, 공격 라벨을 함께 수집할 수 있도록 구성되었다. 또한 MITRE ATT&CK for ICS 기반의 위협 모델을 적용하여 설정값 변조, 비인가 명령, 반복 I/O 조작, 태그 식별, 서비스 거부(DoS), 보고 메시지 위조, 중간자(MitM) 공격 시나리오를 구현하였다. 실험 결과, 공격 유형에 따라 네트워크 계층과 공정 계층에서 관측되는 특성이 상이하였으며, 일부 공격은 패킷 정보만으로 식별하기 어려워 공정 상태 로그와의 연계 분석이 필요함을 확인하였다.

주제어 산업제어시스템, 운영기술, 침입탐지, 수처리 플랜트, 사이버-물리 보안

Ⅰ. 머리말

수처리, 전력, 가스, 교통 등 국가 기반시설의 운영을 담당하는 산업제어시스템(Industrial Control System, ICS)은 센서, 액추에이터, PLC(Programmable Logic Controller), HMI (Human Machine Interface), SCADA(Supervisory Control and Data Acquisition) 시스템을 통해 물리 공정을 감시하고 제어하는 핵심 운영기술(Operational Technology, OT)이다. NIST SP 800-82는 OT를 물리 환경과 상호작용하거나 이를 관리하는 프로그래머블 시스템 및 장치로 정의한다(Stouffer et al. 2023). 과거 ICS는 상대적으로 폐쇄적인 운용 환경을 전제로 설계되었으나, 최근 원격 모니터링과 데이터 기반 운영이 확대되면서 IT 네트워크와의 연계가 증가하고 있다. 이러한 상호연결성은 레거시 ICS에 새로운 공격 표면을 형성하며, 사이버 공격이 정보 유출을 넘어 물리 공정 장애, 설비 손상, 서비스 중단으로 이어질 수 있다는 점에서 일반 IT 시스템과 구별되는 보안 문제를 야기한다(Conti et al. 2021).

수처리 플랜트는 이러한 사이버-물리 보안(Cyber-Physical Security, CPS) 문제를 잘 보여주는 대표적인 OT/ICS 환경이다. 수처리 공정에서는 수위, 유량, pH, 염소 농도와 같은 공정 변수가 지속적으로 측정되며, PLC는 측정값과 제어 로직에 따라 펌프, 밸브, 약품 주입 장치 등의 액추에이터를 제어한다. 기존에도 SWaT(Secure Water Treatment)와 WADI(Water Distribution)와 같은 수처리 기반 테스트베드 및 데이터셋이 제안되어 침입탐지 연구에 활용되어 왔다(Mathur and Tippenhauer 2016; Goh et al. 2017; Ahmed et al. 2017).

ICS 침입탐지 연구에서 데이터셋은 탐지 모델의 학습, 검증, 비교 평가를 위한 핵심 전제이나, 실제 산업 설비에서 공격 데이터를 수집

하는 것은 안전성, 비용, 운영 중단 위험, 법적·윤리적 제약으로 인해 어렵다(Morris and Gao 2014; Lin et al. 2020; Morris et al. 2011; Mathur and Tippenhauer 2016). 기존 수처리 및 ICS 보안 데이터셋은 중요한 연구 기반을 제공하지만, 공개 데이터셋의 경우 공격 시나리오와 수집 구조가 고정되어 있어 통신 주체, 기능 코드, 접근 주소, 요청 주기, 공격 지속시간, 공정 라벨을 연구 목적에 맞게 조정하며 반복 실험을 수행하기에는 한계가 있다. 특히 Modbus/TCP 기반 ICS에서는 동일한 기능 코드라도 송신 주체, 접근 주소, 요청 주기, 쓰기 값, 공정 영향에 따라 정상 행위와 공격 행위의 의미가 달라질 수 있으므로, 네트워크 이벤트와 공정 상태 변화를 동일한 시간축에서 함께 분석할 수 있는 데이터 생성 환경이 필요하다(Gao and Morris 2014).

이러한 필요성에 따라, 본 논문은 수처리 OT/ICS 환경에서 침입탐지 데이터셋 생성을 위한 사이버보안 실험용 시뮬레이터를 설계 및 구현한다. 제안하는 시뮬레이터는 실제 수처리 플랜트의 물리·화학 공정을 정밀하게 복제하는 디지털 트윈이 아니라, 수처리 공정, PLC, HMI, 공격자 노드, Modbus/TCP 통신 구조를 결합하여 네트워크 트래픽, 공정 상태 로그, 공격 라벨, 실험 설정 정보를 함께 생성하는 목적 지향형 실험환경이다.

본 논문의 주요 기여는 세 가지이다. 첫째, 수처리 OT/ICS 환경에서 정상 운전과 공격 시나리오를 반복 수행할 수 있는 목적 지향형 시뮬레이터 구조를 제안한다. 둘째, 정상 운전 시 허용되는 통신 주체, 기능 코드, 접근 대상, 실행 주기를 정의하고, MITRE ATT&CK for ICS를 참고하여 Modbus/TCP 기반 공격 시나리오와 라벨링 기준을 구성한다. 셋째, 네트워크 트래픽과 공정 상태 로그를 함께 분석하여 패킷 기반 탐지만으로는 식별하기 어려운 공정 영향 기반 탐지

의 필요성을 제시한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 ICS 보안 연구에서 활용되어 온 기존 테스트베드, 시뮬레이터 및 데이터셋을 검토하고, 본 논문과의 차별성을 정리한다. Ⅲ장에서는 공정-네트워크 연계형 수처리 플랜트 시뮬레이터의 설계 목표와 범위, 전체 아키텍처, 정상 운전 및 통신 규칙, 데이터 수집 및 산출물 설계를 설명한다. Ⅳ장에서는 위협 모델, 공격 시나리오 설계, 데이터 생성 절차, 라벨링 기준을 제시한다. Ⅴ장에서는 제안한 시뮬레이터를 통해 생성한 정상 운전 데이터와 공격 시나리오별 데이터를 네트워크 특성 및 공정 영향 관점에서 분석한다. Ⅵ장에서는 본 논문의 한계점을 정리하고, Ⅶ장에서는 연구 결과를 요약한 뒤 향후 연구 방향을 제시한다.

Ⅱ. 기존 연구

ICS 보안 연구에서는 실제 설비를 대상으로 공격 데이터를 수집하기 어렵기 때문에 테스트베드, 시뮬레이터, 공개 데이터셋을 활용한 연구가 지속되어 왔다. 특히 침입탐지 관점에서는 네트워크 트래픽뿐만 아니라 공격이 공정 상태와 제어 동작에 미치는 영향을 함께 관측할 수 있는 실험환경이 요구된다.

수처리 및 물 분배 분야에서는 SWaT와 WADI가 대표적인 테스트베드 기반 데이터셋으로 활용되어 왔다(Mathur and Tippenhauer 2016; Goh et al. 2017; Ahmed et al. 2017). 이들 데이터셋은 실제 하드웨어 기반 환경에서 수집되었다는 장점이 있으나, 공개 데이터셋 특성상 공격 시나리오와 수집 조건이 고정되어 있어 연구자가 공격 조건과 정상

운전 규칙을 자유롭게 변경하며 데이터를 반복 생성하기에는 한계가 있다.

MiniCPS와 HAI는 ICS 보안 실험환경 측면에서 중요한 기반을 제공한다. MiniCPS는 물리 공정, 제어 장치, 네트워크 에뮬레이션을 구성할 수 있는 범용 CPS 보안 실험 프레임워크이며(Antonioli and Tippenhauer 2015), HAI는 HIL(Hardware-in-the-Loop) 기반 ICS 테스트베드에서 수집된 정상 및 공격 데이터를 제공한다(Shin et al. 2020). 다만 두 연구 모두 특정 수처리 Modbus/TCP 환경에서 정상 운전 규칙, 공격 라벨, 데이터 생성 절차를 통합적으로 구성하고 반복 실행하는 구조와는 차이가 있다.

BATADAL은 물 분배 네트워크의 SCADA 시계열 데이터를 기반으로 공격 탐지 알고리즘 비교에 활용되어 왔다(Taormina et al. 2018). 그러나 패킷 수준의 네트워크 행위보다 공정 상태 시계열과 탐지 평가에 초점을 두므로, PCAP 기반 네트워크 트래픽과 공정 상태 로그를 함께 생성하려는 본 논문과의 목적이 다르다.

〈표 1〉은 기존 ICS 보안 실험환경 및 데이터셋과 본 논문과의 차이를 데이터 생성 관점에서 비교한 것이다. 기존 연구들은 실제 테스트베드, HIL 기반 데이터셋, CPS 실험 프레임워크 측면에서 중요한 기반을 제공한다. 그러나 정상 운전 규칙, Modbus/TCP 공격 행위, 네트워크 트래픽, 공정 상태 로그, 공격 라벨을 하나의 절차로 통합하여 반복 생성하는 구조는 제한적이다. 본 논문은 이를 보완하기 위해 수처리 공정, PLC-HMI 통신, 공격 시나리오, 라벨링을 통합한 목적 지향형 시뮬레이터를 제안한다.

본 논문은 이를 보완하기 위해 수처리 공정, PLC-HMI 통신, 공격 시나리오, 라벨링을 통합한 목적 지향형 시뮬레이터를 제안한다. 본

논문은 수처리 특화 테스트베드뿐 아니라 범용 ICS·CPS 실험환경을 함께 분석하였다. 이 과정에서 범용 프레임워크는 재사용 가능한 계층 구조와 네트워크 에뮬레이션을 제공하지만, 특정 공정의 정상 운전 규칙·공격 라벨·공정-네트워크 연계 데이터를 통합 생성하는 구조가 제한적이고, 수처리 테스트베드는 실제성이 높으나 공격 조건과 수집 구조가 고정되어 있음을 확인하였다. 이에 본 논문은 범용 실험환경의 계층 분리 구조라는 장점을 유지하면서, 수처리 공정 고유의 물리·화학적 거동을 시나리오 설계와 라벨링에 반영함으로써, 네트워크 트래픽과 공정 상태 로그를 동일 시간축에서 함께 분석할 수 있는 침입탐지 데이터셋을 생성한다.

〈표 1〉 기존 연구와 본 논문의 비교

구분	대상 환경	주요 데이터	장점	한계 및 비교
MiniCPS	CPS/ICS 실험 환경	물리 공정, 제어 장치, 네트워크 에뮬레이션	사용자 정의 실험 환경 구성 가능	수처리 공정, 공격 라벨, 데이터 생성 절차를 별도로 구성해야 함
SWaT	수처리 플랜트	공정 데이터, 네트워크 트래픽, 공격 데이터	실제 하드웨어 기반 수처리 테스트 베드	공개 데이터셋의 공격 조건과 수집 구조 변경이 제한적임
WADI	물 분배 시스템	장기간 정상 및 공격 데이터	물 분배 환경의 이상 탐지 연구	사용자가 공격 조건을 자유롭게 재구성하기 어려움
HAI	HIL 기반 ICS	정상 및 공격 상황의 ICS 데이터	실제 제어 환경을 반영한 데이터 제공	수처리 Modbus/TCP 공격을 반복 주입하는 구조와 차이가 존재함
BATADAL	물 분배 네트워크	SCADA 시계열, 공격 탐지 평가 데이터	공격 탐지 알고리즘 비교에 활용 가능	PCAP 기반 네트워크 행위 분석에는 제한적임
본 논문	수처리 플랜트	PCAP, 공정 상태 로그, 공격 라벨, 실험 설정 정보	정상 운전 및 공격 시나리오의 반복 생성 가능	정밀 공정 해석보다 침입탐지 데이터셋 생성에 초점

Ⅲ. 공정-네트워크 연계형 수처리 플랜트 시뮬레이터 설계

본 장에서는 수처리 OT/ICS 환경에서 침입탐지 데이터셋을 생성하기 위한 시뮬레이터의 설계 구조를 설명한다.

1. 설계 목표 및 범위

본 논문의 시뮬레이터는 수처리 플랜트 환경에서 침입탐지 데이터셋을 반복 생성하기 위한 목적 지향형 실험환경을 모사한다. 따라서 실제 설비의 모든 물리적 특성을 고정밀로 재현하기보다, 보안 실험에 필요한 공정 변수, 제어 명령, 통신 행위, 공격 라벨을 비교 가능한 형식으로 생성하는 데 초점을 둔다.

〈표 2〉 시뮬레이터 설계 목표와 범위

구분	내용
설계 목적	침입탐지 데이터셋 생성을 위한 수처리 OT/ICS 실험환경 구성
대상 공정	3단계 수처리 공정
주요 구성 요소	센서, 액추에이터, PLC, HMI, 공격자 노드
통신 방식	Modbus/TCP 기반 PLC-HMI 통신
주요 산출물	네트워크 트래픽, 공정 상태 로그, 공격 라벨, 실험 설정 정보
설계 범위	정밀 공정 해석보다 보안 실험 및 데이터 생성에 초점

시뮬레이터의 구체적인 설계 목표와 범위를 〈표 2〉에 정리하였다. 본 시뮬레이터는 수처리 공정 변수, PLC-HMI 간 Modbus/TCP 통신, 정상·공격 구간 실행, 네트워크 트래픽 및 공정 상태 로그 산출을

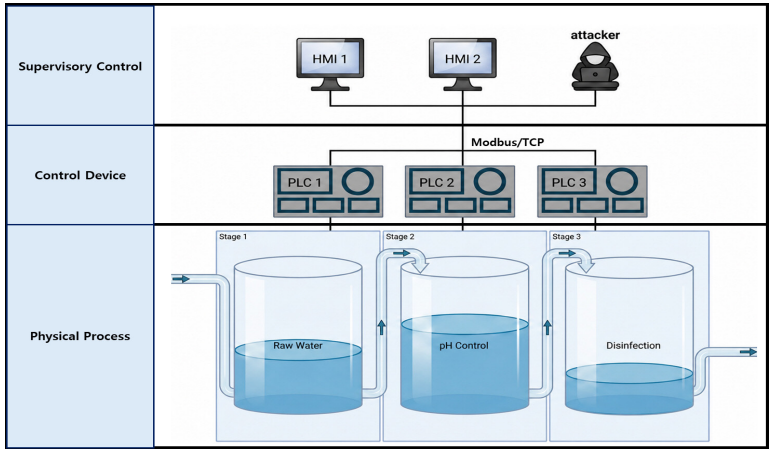
하나의 실험 절차로 통합한다.

공정 범위는 원수 유입 및 이송, pH 조정, 염소 주입 및 출수 제어로 구성된 3단계 수처리 공정으로 한정한다. 이는 실제 수처리 플랜트의 전체 공정을 포괄하기보다 PLC 제어, 센서 측정, 액추에이터 동작, HMI 모니터링, Modbus/TCP 통신을 함께 관측하기 위한 최소 공정 구조이다.

2. 시뮬레이터 아키텍처

제안한 수처리 플랜트 시뮬레이터의 전체 아키텍처가 〈그림 1〉에 나타나 있다. 시뮬레이터는 상위 감시·운영 계층, 제어 장치 계층, 물리 공정 계층의 3계층 구조로 구성되며, HMI, 공격 실험용 노드, PLC, 3단계 수처리 공정이 Modbus/TCP 기반 제어 네트워크를 통해 연결된다.

〈그림 1〉 수처리 플랜트 시뮬레이터 아키텍처



상위 감시·운영 계층은 공정 상태 조회와 제한적 설정값 변경을 담당한다. HMI1은 운영자용 HMI로서 PLC 상태를 주기적으로 조회하고, HMI2는 엔지니어링용 HMI로서 상태 조회와 제한적 설정값 변경을 수행한다. 공격 실험용 노드는 정상 운전 구간에서는 통신하지 않으며, 공격 시나리오 수행 시 PLC를 대상으로 비정상 Modbus/TCP 요청을 발생시키는 주체로 정의하였다.

제어 장치 계층의 PLC1, PLC2, PLC3은 각각 Stage 1, Stage 2, Stage 3의 공정 상태를 관측하고, 사전에 정의된 제어 로직에 따라 액추에이터 동작을 결정한다. HMI-PLC 통신은 Modbus/TCP를 기반으로 하며, 정상 운전 시에는 허용된 상태 조회와 제한적 설정값 변경만 발생하도록 정의하였다.

물리 공정 계층은 원수 유입 및 이송, pH 조정, 염소 주입 및 출수 제어의 3개 Stage로 구성된다. 각 Stage는 대응되는 PLC와 연결되며, PLC는 수위, 유량, pH, 염소 농도 등의 센서 값을 기반으로 펌프, 밸브, 약품 주입 장치의 동작을 제어한다.

본 시뮬레이터는 수처리 공정에 특화된 화학·안전 요건을 모델에 적극 반영하였다. 구체적으로 Stage 2에서는 $[H^+]$ 상태와 약품 주입에 따른 pH의 비선형 변화를 모사하며, Stage 3에서는 자유염소 잔류(Cf)에 대한 질량수지와 pH 의존적 $HOCl/OCl^-$ 분배를 구현하여 살균력 차이의 근거가 되는 화학적 거동을 표현한다. 나아가 공정 이상(process anomaly) 라벨에는 잔류염소 부족, CT 부족, pH 안전 범위 이탈 등 수처리 환경에 특화된 분류 어휘를 포함한다. 이러한 요소는 수처리 공정의 운영 특성과 수질 안전 요구사항을 반영하기 위한 것으로, 공정 상태 변화와 이상 상황을 현실적으로 표현할 수 있도록 하였다.

본 시뮬레이터의 PLC, HMI, 공격자 노드는 모두 자체 구현하였다.

PLC 제어 로직은 Python 기반 모듈로 작성하였으며, Stage 1, Stage 2, Stage 3에 대응하는 제어 로직을 각각 분리하여 구성하였다. 각 PLC는 센서 입력값을 기반으로 제어 판단을 수행하고, 펌프·밸브·약품 주입 장치와 같은 액추에이터의 명령 상태를 갱신한다. HMI는 운영자용 HMI와 엔지니어링용 HMI로 구분하여 자체 컨테이너로 구현하였으며, 운영자용 HMI는 주기적 상태 조회를, 엔지니어링용 HMI는 상태 조회와 제한적 설정값 변경을 수행한다. 공격자 노드는 별도 컨테이너로 구성하여 OT 가상 네트워크에 연결하였고, 실제 Modbus/TCP 요청을 발생시켜 PCAP에 공격 트래픽이 기록되도록 하였다. 본 논문에서는 OpenPLC와 같은 기존 PLC/HMI 에뮬레이터를 사용하지 않고, 보안 실험 목적에 맞게 PLC·HMI·공격자 구성 요소를 직접 구현하였다.

이와 같은 아키텍처는 정밀 공정 해석보다 공정 상태, PLC 제어 동작, HMI 조회, Modbus/TCP 통신 행위를 동일한 실험 환경에서 관측하기 위한 구조이다. 이를 통해 정상 통신 기준선을 설정하고, 공격 시나리오 수행 시 네트워크 행위와 공정 상태 변화의 관계를 분석할 수 있다. 각 Stage의 주요 기능, 공정 변수, 제어 대상을 〈표 3〉에 정리하였다. 이는 정상 운전 기준과 공격 발생 시 공정 영향 분석의 기준으로 활용된다.

〈표 3〉 수처리 공정 단계별 구성 요소

공정 단계	주요 기능	공정 변수	제어 대상
Stage 1	원수 유입 및 이송	수위, 유입 유량	유입 밸브, 이송 펌프
Stage 2	pH 조정	수위, 유량, pH	약품 주입 밸브, 이송 펌프
Stage 3	염소 주입 및 출수	수위, 출수 유량, 염소 농도	염소 주입 밸브, 출수 밸브, 배수 펌프

3. 정상 운전 및 통신 규칙

정상 운전 시 각 PLC는 대응 Stage의 센서 값을 기반으로 제어 명령을 생성하고, 펌프, 밸브, 약품 주입 장치의 동작 상태를 결정한다. 액추에이터 제어는 PLC 제어 로직에 의해 수행되며, 외부 노드가 액추에이터 코일을 직접 쓰는 동작은 정상 통신 규칙에서 제외한다.

정상 운전 시 PLC는 각 Stage의 센서 값을 기반으로 제어 명령을 생성한다. PLC1은 Stage 1의 원수 유입 및 이송을 제어하고, PLC2는 Stage 2의 pH 조정 공정을 제어하며, PLC3은 Stage 3의 염소 주입 및 출수 제어를 담당한다. 각 PLC는 수위, 유량, pH, 염소 농도와 같은 공정 변수를 입력으로 사용하고, 펌프, 밸브, 약품 주입 장치와 같은 제어 대상의 동작 상태를 결정한다. 정상 운전에서 액추에이터 제어는 PLC의 제어 로직에 의해 수행되며, 외부 노드가 액추에이터 코일을 직접 쓰는 동작은 정상 통신 규칙에 포함하지 않았다.

HMI는 운영자용 HMI1과 엔지니어링용 HMI2로 구분된다. HMI1은 PLC 상태를 주기적으로 조회하고, HMI2는 상태 조회와 제한적 설정값 변경을 수행한다. 이에 따라 정상 운전 중 HMI 통신은 코일 및 레지스터 조회를 중심으로 구성되며, 설정값 변경은 HMI2에 한정된다. 정상 통신에서는 HMI1과 HMI2의 FC01·FC03 기반 상태 조회와 HMI2의 제한적 FC06 설정값 변경만 허용하였다. 반면 FC05 요청, 공격자 노드의 PLC 대상 요청, 비정상적으로 높은 요청 빈도, ARP 기반 경로 조작은 정상 통신 행위에서 제외하였다.

이러한 정상 운전 및 통신 규칙은 〈표 4〉와 같이 이후 공격 시나리오 정의와 라벨링의 기준으로 사용된다. 동일한 기능 코드라도 송신 주체, 접근 주소, 요청 주기, 쓰기 값, 공정 영향에 따라 정상 행위와

공격 행위의 의미가 달라질 수 있으므로, 본 논문에서는 기능 코드뿐만 아니라 통신 맥락과 공정 상태 변화를 함께 고려하여 정상 기준선을 정의하였다.

〈표 4〉 정상 운전 시 HMI-PLC 통신 규칙

통신 주체	대상	주요 기능 코드	정상 행위
HMI1	PLC1, PLC2, PLC3	FC01, FC03	코일 및 레지스터 상태 조회
HMI2	PLC1, PLC2, PLC3	FC01, FC03, FC06	상태 조회 및 제한적 설정값 변경
PLC1, PLC2 ,PLC3	HMI1, HMI2	응답 패킷	HMI 요청에 대한 상태 응답
공격자 노드	-	-	정상 운전 구간에서는 통신 없음

정상 운전 규칙은 공격 행위를 판별하기 위한 행위 기준선으로 기능한다. 본 논문은 이를 기준으로 정상 데이터와 공격 데이터를 구분하고, 네트워크 트래픽과 공정 상태 로그를 동일 시간축에서 비교하도록 구성하였다.

4. 데이터 수집 및 산출물 설계

본 시뮬레이터는 침입탐지 데이터셋 생성을 위해 네트워크 행위와 공정 상태 변화를 동일한 실험 시간 축에서 수집하도록 설계하였다. 수집 데이터는 네트워크 트래픽, 공정 상태 로그, 공격 라벨, 실험 설정 정보로 구분되며, 이를 통해 특정 네트워크 이벤트와 공정 변수·제어 동작의 관계를 함께 분석할 수 있다.

네트워크 트래픽은 HMI, PLC, 공격자 노드 사이의 Modbus/TCP

통신을 포함하며, 패킷 단위 분석을 위해 PCAP 형식으로 저장된다. 이를 통해 통신 주체, 기능 코드, 접근 주소, 요청 주기, 쓰기 값 등을 정상 통신 규칙과 비교하여 비인가 요청과 비정상 통신 패턴을 식별할 수 있다.

공정 상태 로그는 각 Stage의 수위, 유량, pH, 염소 농도와 같은 공정 변수와 PLC 제어 명령, 액추에이터 상태를 시간 순서대로 기록한다. 이를 통해 네트워크상 제어 요청이 실제 공정 변화로 이어졌는지, 또는 센서 측정값과 실제 상태 사이에 불일치가 발생했는지를 분석할 수 있다.

공격 라벨은 정상·공격 구간을 구분하고 공격 유형, 대상 장치 또는 Stage, 공격 시작·종료 시점, 관측 계층을 식별하기 위한 기준 정보로 사용된다. 공격 유형별 세부 라벨링 기준은 Ⅳ장에서 설명한다.

실험 설정 정보는 실험 시간, 정상 운전 구간, 공격 주입 시점, 공격 지속시간, 대상 장치, 통신 조건, 시나리오 식별 정보를 포함하며, 동일 조건의 반복 실험과 시나리오 간 비교를 위한 재현성 기준으로 활용된다. 〈표 5〉는 본 논문에서 생성되는 주요 산출물과 활용 목적을 정리한 것이다. 네트워크 트래픽은 패킷 기반 탐지에, 공정 상태 로그는 물리적 영향 분석에, 공격 라벨은 학습·평가 기준에, 실험 설정 정보는 재현성 확보에 활용된다.

〈표 5〉 시뮬레이터 산출 데이터와 활용 목적

산출 데이터	주요 내용	활용 목적
공정 상태 로그	Stage별 공정 상태, PLC 제어 명령, 액추에이터 상태	정상 운전 및 공격 시 공정 상태 변화 분석
네트워크 트래픽	HMI-PLC 및 공격자-PLC 간 Modbus/TCP 패킷	정상 통신과 공격 행위의 네트워크 증거 분석

산출 데이터	주요 내용	활용 목적
공격 라벨	공격 유형, 공격 시작·종료 시점, 대상 장치 또는 Stage	정상/공격 구간 구분 및 공격 영향 분석
실험 설정 정보	시나리오 조건, 실행 시간, 대상 PLC, 대상 공정 단계	반복 실험 및 결과 비교 기준 제공

데이터셋의 구체적 형식을 명확히 하기 위해 공정 상태 로그와 네트워크 트래픽의 기록 구조를 구분하여 정의하였다. 〈표 6〉은 본 논문에서 생성한 공정 상태 로그 CSV의 컬럼 구조를 나타낸다. 공정 상태 로그는 1초 단위의 시뮬레이션 스냅샷을 기준으로 시간 키, 실제 공정 상태, 센서 측정값, 액추에이터 명령 및 동작 상태, 라벨 정보를 포함한다.

〈표 6〉 공정 상태 로그 CSV 컬럼 구조

구분	주요 컬럼 예시	설명
시간 정보	t_sim_s, tick, scan_idx, hmi_poll_idx	시뮬레이션 시간 및 수집 주기 식별
공정 상태	V1_m3, V2_m3, V3_m3, h1_m, h2_m, h3_m	공정 상태 및 주요 물리 및 화학 변수
센서 측정	LIT101_meas, FIT101_meas, AIT201_meas	HMI와 PLC가 관측하는 센서 측정 값
액추에이터 상태	MV101_cmd/act, P101_cmd/act, MV201_cmd/act	PLC 명령 상태와 액추에이터 동작 상태
라벨	mode, attack_active, attack_type, attack_target, attack_stage	공격 여부, 공격 유형, 대상, 공정 이상 및 관측 계층 정보

한편, 네트워크 트래픽은 PCAP 형식으로 저장되며, Modbus/TCP

패킷의 주요 필드를 기준으로 기능 코드와 접근 대상을 추출하였다. 〈표 7〉은 본 논문에서 사용한 Modbus/TCP PCAP 파싱 기준을 정리한 것이다. 특히 Function Code 필드는 정상 조회 요청과 공격성 쓰기 요청을 구분하는 핵심 기준으로 활용된다.

〈표 7〉 Modbus/TCP PCAP 파싱 기준

바이트 오프셋	필드	설명
0-5	MBAP Header	Transcation ID, Protocol ID, Length로 구성되는 Modbus/TCP Header
6	Unit ID	대상 슬레이브 또는 PLC 식별자
7	Function Code	주요 추출 대상 Function code: FC01. FC03, FC05, FC06 등
8 이후	Data	Function code별 접근 주소, 요청 길이, 쓰기 값 등 가변 데이터 영역

따라서, 본 데이터셋은 공정 상태 로그와 네트워크 트래픽을 서로 다른 형식으로 저장하되 동일한 실험 시간축에서 연계할 수 있도록 구성하였다. 예를 들어 설정값 변조 공격의 경우 PCAP에서는 FC06 요청 증가가 관측되고, 공정 상태 로그에서는 해당 설정값 변경 이후 pH 또는 염소 농도 관련 변수 변화가 관측될 수 있다. 따라서 본 데이터 형식은 패킷 기반 분석뿐만 아니라 공정 상태 기반 분석, 나아가 두 계층을 결합한 침입탐지 연구에 활용될 수 있다.

따라서 본 논문의 데이터 수집 구조는 단일 계층 관측 방식과 구별된다. 네트워크 트래픽, 공정 상태 로그, 공격 라벨을 동일 시간축에서 생성함으로써 Modbus/TCP 기반 공격 행위와 공정 변화의 관계를 분석할 수 있으며, 이는 이후 공격 시나리오 설계와 실험 결과 분석의 기반이 된다.

Ⅳ. 공격 시나리오 및 데이터 생성

본 장에서는 Ⅲ장에서 정의한 시뮬레이터 구조와 정상 운전 규칙을 기반으로 공격 시나리오와 데이터 생성 절차를 설명한다.

1. 위협 모델

본 논문의 위협 모델은 〈표 8〉과 같이 수처리 OT/ICS 제어 네트워크 내부에 비인가 노드가 존재하는 상황을 가정한다. 공격자는 외부 인터넷에서 PLC에 직접 접근하는 원격 행위자가 아니라, 제어 네트워크 내부에 진입했거나 내부 호스트를 장악한 행위자로 정의한다. 이에 따라 공격자는 HMI-PLC 간 Modbus/TCP 통신 구간에 접근하여 읽기·쓰기 요청, 반복 요청, 주소 스캔, ARP 기반 경로 개입을 수행할 수 있다.

〈표 8〉 위협 모델 구성 요소

구분	내용
공격자 위치	제어 네트워크 내부
공격자 권한	PLC 펌웨어 및 물리 설비에 대한 직접 권한은 없으나 Modbus/TCP 요청 생성 가능
공격 가능 행위	레지스터 쓰기, 코일 쓰기, 반복 읽기 요청, 센서 측정값 변조, ARP spoofing
공격 대상	설정값 레지스터, 액추에이터 코일, 센서 측정값, HMI-PLC 통신 경로
주요 관측 데이터	네트워크 트래픽, 공정 상태 로그, 공격 라벨
제외 범위	초기 침투, PLC 펌웨어 변조, 물리 설비 파괴, 실제 수처리 플랜트의 정밀 공정 해석

공격자의 목표는 수처리 공정의 정상 제어 흐름을 교란하거나 침입탐지 관점에서 의미 있는 비정상 행위를 발생시키는 것이다. 구체적으로 공격자는 설정값 레지스터 변경, 액추에이터 코일에 대한 비인가 쓰기, 레지스터·코일 주소 스캔, 고빈도 반복 요청, 센서 측정값 불일치 유발, HMI-PLC 통신 경로 개입을 수행할 수 있다.

본 논문에서 공격자는 PLC 펌웨어를 직접 변조하거나, 물리 설비를 직접 조작하는 고도 권한을 가진 행위자로 가정하지 않는다. 또한 운영자의 정상 행위 자체를 악의적으로 재정의하지 않으며, 정상 운전 구간에서는 HMI1과 HMI2가 Ⅲ장에서 정의한 통신 규칙에 따라 동작하는 것으로 가정한다. 따라서 공격 행위는 정상 통신 규칙에서 벗어나는 송신 주체, 기능 코드, 접근 주소, 요청 주기, 쓰기 값, 또는 공정 상태 불일치를 통해 식별된다.

본 논문의 공격 대상은 설정값 레지스터, 액추에이터 코일, 센서 측정값, HMI-PLC 통신 경로로 구분된다. 설정값 레지스터는 pH 또는 염소 농도와 같은 제어 목표값 변조를 관측하기 위한 대상이다. 액추에이터 코일은 펌프·밸브에 대한 비인가 쓰기 요청과 정상 제어 로직의 충돌을 관측하기 위한 대상이다. 센서 측정값은 수위, 유량, pH, 염소 농도 등 실제 공정 상태와 표시·제어 상태 간 불일치를 분석하기 위한 대상이다. HMI-PLC 통신 경로는 ARP 기반 경로 개입과 MAC-IP 매핑 변화를 관측하기 위한 대상이다.

본 논문의 위협 모델은 사전에 정의한 공격 유형만을 고정적으로 실행하는 구조가 아니라, 연구자가 공격 조건을 변경하며 새로운 시나리오를 구성할 수 있도록 설계하였다. 〈표 9〉은 본 시뮬레이터에서 위협 모델을 확장하기 위해 제공하는 주요 인터페이스를 정리한 것이다. 연구자는 센서 측정값 편차, 액추에이터 강제 상태, 설정값 변

경, 공격 지속시간, 공격 대상 등을 조정할 수 있으며, 이를 통해 동일한 공격 유형 내에서도 서로 다른 네트워크 및 공정 영향을 갖는 데이터를 생성할 수 있다. 또한, 본 연구의 위협 모델은 단일 공격 목록을 재현하는 데 그치지 않고 공격 조건을 조정할 수 있는 확장형 구조를 갖는다. 특히 공격자 노드, 기능 코드, 접근 주소, 요청 주기, 공격 지속시간을 변경할 수 있으므로, 기존 공개 데이터셋에서 제한되는 고정 시나리오 문제를 완화하고 연구 목적에 따라 다양한 공격 데이터를 반복 생성할 수 있다.

〈표 9〉 위협 모델 확장 인터페이스

구분	변경 가능한 요소	활용 목적
센서 측정값 편차	임의 센서와 bias 값	실제 상태와 측정 상태 간 불일치 발생
액추에이터 강제 상태	펌프, 밸브 등 액추에이터 ON/OFF	비인가 제어 명령 및 반복 I/O 조작 재현
설정값 변경	pH, 염소 농도 등 제어 목표 값	공정 제어 목표 변조와 후속 공정 변화 분석
외부 공격 입력	공격자 노드, 대상 주소, 요청 주기	통신 주체, 기능 코드, 접근 주소, 요청 빈도 변화 실험
시나리오 선언	공격 시작 시점, 지속시간, 대상, 공격 유형	동일 조건의 반복 실행 및 재현

본 논문은 공격 행위를 네트워크 계층과 공정 계층의 관측 가능성에 따라 구분한다. Modbus/TCP 기능 코드, 송수신 주체, 접근 주소, 요청 빈도는 네트워크 계층의 주요 단서이며, 센서 측정값 불일치와 같이 패킷만으로 식별하기 어려운 공격은 공정 상태 로그를 통해 관측한다. 따라서 본 위협 모델은 단일 패킷의 정상·비정상 여부가 아니라 네트워크 이벤트와 공정 상태 변화를 함께 고려한다.

다만 위협 모델은 침입탐지 데이터셋 생성을 위한 실험 범위에 한정되며, 실제 수처리 시설에서 가능한 모든 공격 경로를 포괄하지 않는다. 물리 장비 파손, 장기간 잠복, 운영자 계정 탈취, PLC 펌웨어 변조, 안전 계장 시스템 우회와 같은 고도 공격은 제외하였으며, 중간자 공격 역시 통신 경로 개입 여부의 관측에 초점을 두고 실제 Modbus 응답 내용 변조는 포함하지 않았다. 이는 공격자 능력을 과도하게 확장하지 않으면서 데이터 생성에 필요한 대표적인 네트워크 및 공정 이상 행위를 통제된 조건에서 재현하기 위한 범위 설정이다.

2. 공격 시나리오 설계

이 절에서는 III장에서 정의한 정상 운전 및 통신 규칙을 기준으로 비정상 행위를 공격 시나리오로 구성하였다. 각 시나리오는 공격 주체, 대상 PLC, 기능 코드, 접근 주소, 요청 주기, 공정 영향 여부를 기준으로 구분하였다. 공격 유형은 MITRE ATT&CK for ICS의 기법을 참고하여 선정하였으며, 정상 통신 규칙에서 벗어나는 쓰기 요청, 고빈도 반복 요청, 주소 탐색, 센서 측정값 불일치, 통신 경로 개입을 포함한다.

공격 시나리오 선정 기준은 세 가지이다. 첫째, Modbus/TCP 환경에서 기능 코드, 요청 빈도, 주소 접근 패턴, ARP 패킷 등 네트워크 계층의 관측 단서를 남길 수 있어야 한다. 둘째, 수위, pH, 염소 농도, 액추에이터 상태와 같은 공정 변수에 직접 또는 간접적인 영향을 줄 수 있어야 한다. 셋째, 특정 기능 코드만으로 정상·비정상을 단순 구분하기보다 송신 주체, 접근 주소, 요청 주기, 쓰기 값, 공정 영향에 따라 공격 의미가 달라지는 사례를 포함해야 한다. 이에 따라 본 연구는

MITRE ATT&CK for ICS의 기법 중 Modbus/TCP 기반 수처리 OT/ICS 환경에서 재현 가능하고 네트워크·공정 계층의 관측 차이를 비교할 수 있는 7개 공격 유형을 선정하였다.

〈표 10〉은 선정된 공격 유형의 MITRE ID, 주요 대상, 공격 행위, 관측 계층을 정리한 것이다. 선정된 공격 시나리오는 관측 계층에 따라 네트워크·공정 동시 관측형, 네트워크 중심형, 공정 중심형으로 구분된다. Modify Parameter, Unauthorized Command Message, Brute Force I/O는 쓰기 요청과 공정 변화가 함께 나타나는 유형이며, Point & Tag Identification, Denial of Service, Adversary-in-the-Middle은 주로 요청 패턴 또는 ARP 계층 변화로 관측된다. Spoof Reporting Message는 기능 코드 변화보다 실제 상태와 측정 상태 간 불일치가 핵심 단서가 되는 공정 중심 공격이다.

다만 Spoof Reporting Message는 실제 Modbus 응답 패킷 위조가 아니라 센서 측정값에 편차를 부여하는 방식으로, Adversary-in-the-Middle은 Modbus 페이로드 변조가 아니라 ARP 기반 통신 경로 개입으로 구현하였다. 이는 공격별 관측 가능성을 명확히 구분하고, 데이터셋 생성에 필요한 네트워크 및 공정 이상 행위를 통제된 조건에서 수집하기 위한 범위 설정이다.

〈표 10〉 공격 시나리오 목록

공격 유형	MITRE ID	주요 대상	공격 행위	관측 계층
Modify Parameter	T0836	설정값 레지스터	FC06을 이용한 pH 또는 염소 설정값 변경	네트워크+공정
Unauthorized Command Message	T0855	액추에이터 코일	FC05를 이용한 펌프·밸브 직접 조작	네트워크+공정

공격 유형	MITRE ID	주요 대상	공격 행위	관측 계층
Brute Force I/O	T0806	액추에이터 코일	동일 코일에 대한 고빈도 ON/OFF 쓰기	네트워크+공정
Point & Tag Identification	T0861	레지스터·코일 주소 영역	FC01·FC03 기반 순차 주소 조회	네트워크
Denial of Service	T0814	PLC 통신 처리	FC03 요청의 고빈도 반복	네트워크
Spoof Reporting Message	T0856	센서 측정값	실제 상태와 측정 상태의 불일치 유발	공정
Adversary-in-the-Middle	T0830	HMI-PLC 통신 경로	ARP 기반 통신 경로 개입	네트워크

3. 데이터 생성 절차

본 논문의 데이터 생성 절차는 〈그림 2〉와 같이 실험 환경 초기화, 정상 운전 구간 수집, 공격 시나리오 실행, 데이터 기록, 라벨링, 침입 탐지 데이터셋 구성의 순서로 수행된다. 이 절차는 정상 구간과 공격 구간을 동일한 흐름에서 생성하여 네트워크 행위와 공정 상태를 비교 가능하게 구성한 것이다.

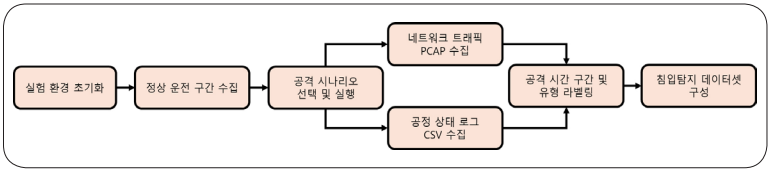
환경 초기화 단계에서는 공정 상태와 통신 상태를 초기 조건으로 설정하고, 정상 운전 구간에서는 공격을 주입하지 않은 상태에서 네트워크 트래픽과 공정 상태 로그를 기록하여 기준 데이터를 구성한다.

정상 구간 수집 이후에는 사전에 정의한 공격 시나리오를 실행하고, 공격 구간의 네트워크 트래픽은 PCAP 형식으로, 공정 상태 로그는 CSV 형식으로 저장한다. 두 데이터는 동일한 실험 시간축에서 생성되므로 공격 발생 전후의 네트워크 행위와 공정 상태 변화를 함께

확인할 수 있다.

공격 실행 이후에는 공격 시간 구간과 공격 유형을 기준으로 라벨을 부여하고, PCAP 파일, 공정 상태 로그, 공격 라벨을 결합하여 침입탐지 데이터셋을 구성한다. 이 절차는 공격 시나리오별 데이터를 동일한 방식으로 생성하고, 정상 데이터와 공격 데이터를 비교 가능한 형태로 정리함으로써 패킷 기반 특징과 공정 상태 변화를 연계한 침입탐지 분석에 활용될 수 있다.

〈그림 2〉 데이터 생성 절차



4. 라벨링 기준

본 연구에서는 공격 시나리오의 실행 시간, 공격 유형, 공격 대상, 관측 채널을 기준으로 라벨을 부여하였다. 정상 구간은 공격이 주입되지 않은 시간 구간으로, 공격 구간은 각 시나리오의 시작 시점부터 종료 시점까지로 정의하였다. 라벨은 네트워크 트래픽과 공정 상태 로그를 동일한 시간 기준에서 연결하고, 공격 유형별 관측 특성을 반영하기 위한 기준 정보로 사용된다. 〈표 11〉은 공격 시나리오별 주요 라벨링 기준을 정리한 것으로, 기능 코드, 대상 주소 또는 상태, 공격 주체, 관측 채널을 기준으로 구성하였다. 〈표 11〉의 관측 채널은 공격 단서가 나타나는 계층을 의미한다. 네트워크·공정 공격은 패킷상의

비정상 행위와 공정 상태 변화가 함께 관측되는 유형이며, 네트워크 중심 공격은 기능 코드, 요청 빈도, 주소 접근 패턴, ARP 패킷을 기준으로 구분된다. 공정 중심 공격은 실제 상태와 측정 상태 간 불일치를 주요 기준으로 라벨링한다.

〈표 11〉 공격 시나리오별 라벨링 기준

공격 유형	주요 라벨 기준	관측 채널
Modify Parameter	FC 06 요청, 대상 Holding Register, 쓰기값, 공격자 출발지	네트워크+공정
Unauthorized Command Message	FC 05 요청, 대상 코일, 강제 ON/OFF 값, 공격자 출발지	네트워크+공정
Brute Force I/O	FC 05 반복 요청, 동일 코일 대상 짧은 요청 주기	네트워크+공정
Point & Tag Identification	FC 01/03 요청, 연속 주소 조회, 넓은 주소 범위 접근	네트워크
Denial of Service	FC 03 요청 폭주, 높은 pps, 동일 대상 반복 접근	네트워크
Spoof Reporting Message	센서 측정값 bias, 실제 상태와 측정 상태의 불일치	공정
Adversary-in-the-Middle	ARP 패킷 증가, MAC-IP 매핑 충돌, HMI-PLC 경로 개입	네트워크

라벨 필드는 공격 여부, 공격 유형, 대상 장치, 대상 주소, 공격 값, 공격 시간, 관측 가능 계층을 포함하며, 〈표 12〉는 그 구성 예시를 나타낸다. 이는 생성된 데이터셋을 패킷 단위 분석과 공정 상태 기반 분석에 모두 활용하기 위한 것이다. 이와 같은 라벨링 기준은 공격 시나리오별 관측 특성을 일관된 형식으로 표현하기 위한 것이다. 동일한 기능 코드라도 송신 주체, 대상 주소, 요청 주기, 쓰기 값, 공정 상태 변화에 따라 정상 행위와 공격 행위가 달라질 수 있으므로, 본 연구는 시간 정보와 관측 채널 정보를 함께 포함하여 네트워크 기반 및 공정

상태 기반 침입탐지 분석에 활용할 수 있도록 하였다.

〈표 12〉 라벨 필드 구성 예시

필드	설명
label_binary	정상은 0, 공격은 1로 표시
attackt_type	공격 시나리오 이름
mitre_id	MITRE ATT&CK for ICS 기법 ID
target_device	공격 대상 PLC 또는 HMI
target_address	공격 대상 레지스터, 코일 또는 센서 태그
attack_value	쓰기 값, bias 값, 토글 패턴 등
start_time	공격 시작 시점
end_time	공격 종료 시점
observable_on_network	네트워크 트래픽에서 관측 가능 여부
observable_on_process	공정 상태 로그에서 관측 가능 여부

V. 실험 결과 및 분석

본 장에서는 제안한 시뮬레이터를 통해 생성한 정상 운전 데이터와 공격 시나리오별 데이터를 네트워크 트래픽 및 공정 상태 로그 관점에서 비교 분석한다. 실험 환경은 물리 공정 및 제어 로직을 실행하는 Python 기반 시뮬레이션 환경과 PLC·HMI·공격자 노드 간 Modbus/TCP 통신을 재현하는 Docker Compose 기반 OT 가상 네트워크로 구성하였다. 공격 트래픽 생성에는 pymodbus와 Scapy를, 패킷 캡처에는 tcpdump를 활용하여 PCAP 형식으로 저장하였다.

1. 정상 운전 구간 분석

정상 운전 구간은 공격이 주입되지 않은 상태에서 수집한 기준 데이터로, 이후 공격 구간과의 비교에 사용하였다. 약 12시간 동안 총 974,199개의 패킷이 수집되었으며, 평균 패킷 발생률은 22.55 pps로 나타났다. 정상 운전 구간의 Modbus/TCP 기능 코드 분포는 〈표 13〉과 같다. FC01과 FC03이 대부분을 차지하였고, FC06은 엔지니어링용 HMI의 제한적 설정값 변경 과정에서 소량 관측되었다. 〈표 13〉의 결과는 정상 운전 구간이 읽기 요청 중심의 통신 패턴을 보이며, FC05가 관측되지 않았음을 보여준다. 이는 이후 공격 구간에서 비인가 코일 쓰기 요청을 식별하는 기준으로 활용될 수 있으나, 본 연구의 실험 조건에서 정의한 정상 운전 규칙에 따른 결과이므로 모든 Modbus/TCP 기반 ICS에 일반화되는 기준은 아니다.

〈표 13〉 장시간 정상 운전 데이터 Modbus/TCP 기능 코드 분포

기능 코드	의미	패킷 수	비율
FC01	Read Coils	259,188	39.91%
FC03	Read Holding Register	388,784	59.86%
FC05	Write Single Coil	0	0%
FC06	Write Single Register	1,494	0.23%

또한 정상 운전 구간에서는 공격자 노드의 PLC 대상 요청과 ARP 기반 경로 조작이 관측되지 않았다. 따라서 공격 구간에서 비인가 노드의 Modbus/TCP 요청, 과도한 요청 빈도, ARP 패킷 증가가 나타나는 경우 이를 정상 기준선과 구분되는 네트워크 특성으로 해석하였다.

2. 공격 시나리오별 네트워크 특성

본 절에서는 공격 시나리오별 대표 구간에서 수집된 PCAP을 기반으로 네트워크 트래픽 특성을 분석한다. 분석 항목은 Modbus/TCP 기능 코드 분포, 요청 빈도, 접근 주소 패턴, 공격자 출발지 여부, ARP 패킷 발생 여부로 구성하였다.

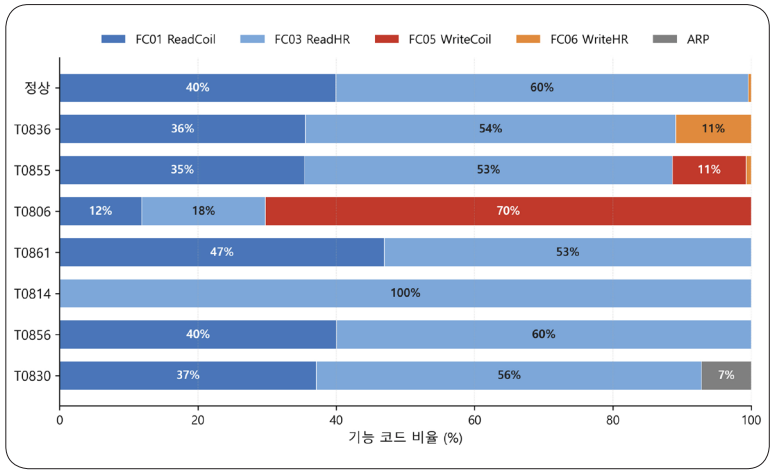
〈표 14〉과 〈그림 3〉은 공격 유형별 네트워크 특성이 기능 코드, 요청 빈도, 주소 접근 패턴, ARP 발생 여부에 따라 구분됨을 보여준다. 쓰기 기반 공격군은 허용되지 않은 FC05 또는 FC06 요청의 출현과 반복성을 주요 단서로 가진다. Modify Parameter는 설정값 레지스터에 대한 FC06 증가로, Unauthorized Command Message와 Brute Force I/O는 액추에이터 코일 대상 FC05 증가로 구분되며, 특히 Brute Force I/O는 동일 코일에 대한 반복 토글로 인해 요청 빈도가 두드러진다.

〈표 14〉 공격 시나리오별 네트워크 트래픽 관측 결과

공격 유형	총 패킷 수	FC01	FC03	FC05	FC06	ARP	주요 네트워크 특성
정상 운전	1,353	360	540	0	2	0	주기적 상태 조회
Modify Parameter	1,678	396	596	0	122	0	FC06 반복 쓰기
Unauthorized Command Message	1,716	404	606	122	8	0	FC05 비인가 쓰기
Brute Force I/O	5,034	398	600	2,354	0	0	FC05 반복 토글
Point & Tag Identification	4,387	1,372	1,550	0	0	0	주소 순차 조회
Denial of Service	695,898	396	695,001	0	0	0	FC03 대량 요청

공격 유형	총 패킷 수	FC01	FC03	FC05	FC06	ARP	주요 네트워크 특성
Spoof Reporting Message	1,491	398	596	0	0	0	관측 불가
Adversary-in-the-Middle	1,969	408	612	0	0	79	ARP 패킷 증가 및 MAC-IP 매핑 충돌

〈그림 3〉 공격 시나리오별 네트워크 패킷 분포



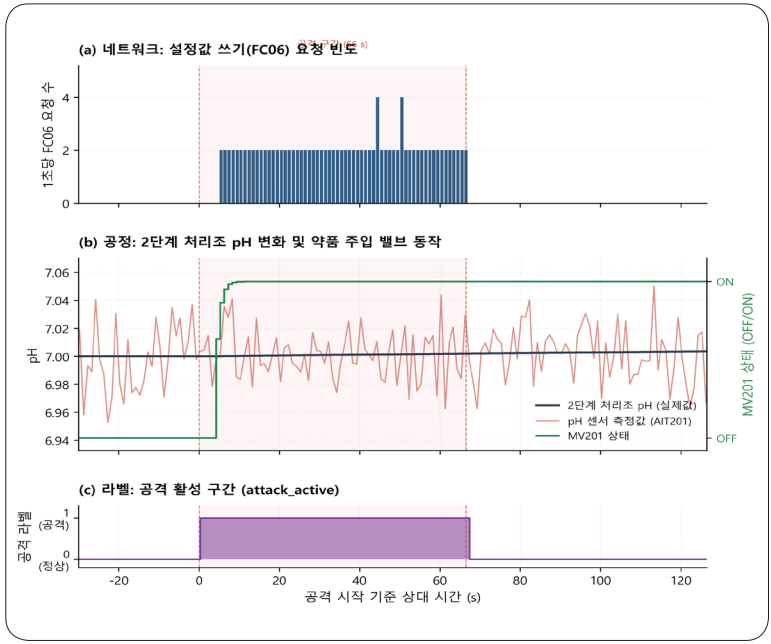
읽기·트래픽 기반 공격군은 FC01 또는 FC03 요청 증가로 관측되지만, 세부적으로는 주소 접근 범위와 요청 빈도에서 차이를 보인다. Point & Tag Identification은 넓은 주소 영역을 순차 조회하는 정찰성 패턴을 보인 반면, Denial of Service는 특정 읽기 요청이 고빈도로 반복되는 폭주성 패턴으로 나타났다.

반면 Spoof Reporting Message는 기능 코드 분포가 정상 구간과 유사하게 나타나 네트워크 트래픽만으로 식별하기 어렵고, 공정 상태 로그에서의 측정값 불일치를 함께 확인해야 한다. Adversary-in-the-Middle 역시 Modbus/TCP 기능 코드 분포보다 ARP 패

킷 증가와 MAC-IP 매핑 변화가 핵심 단서로 나타나므로, 기능 코드 중심 분석만으로는 충분하지 않다. 따라서 네트워크 기반 분석에서는 기능 코드뿐만 아니라 요청 빈도, 주소 접근 범위, 송신 주체, ARP 계층 변화를 함께 고려해야 하며, 네트워크 단서가 제한적인 공격은 공정 상태 로그와 결합하여 해석할 필요가 있다.

네트워크 트래픽과 공정 상태 로그의 시간적 연계성을 확인하기 위해 Modify Parameter 공격 구간을 대상으로 기능 코드 변화와 공정 변수 변화를 동일 시간축에서 비교하였다. 〈그림 4〉는 공격 발생 전후의 FC06 요청 빈도, pH 관련 공정 변수, 공격 라벨을 함께 나타낸 것이다. 이를 통해 네트워크 계층에서 관측되는 설정값 쓰기 요청이 공정 계층의 상태 변화와 어떤 시간적 관계를 갖는지 확인할 수 있다. 이와 같이, Modify Parameter 공격 구간에서는 FC06 요청 빈도가 증가하는 시점과 공격 라벨이 활성화되는 시점이 대응된다. 이후 공정 상태 로그에서는 pH 관련 변수의 변화가 관측되며, 이는 네트워크상의 설정값 변경 요청이 공정 상태 변화로 이어질 수 있음을 보여준다. 이와 같은 결과는 단일 패킷 또는 단일 공정 변수만을 분석하는 방식보다, PCAP 기반 네트워크 특징과 CSV 기반 공정 상태 로그를 동일 시간축에서 결합하는 방식이 공격 의미 해석에 효과적임을 시사한다.

〈그림 4〉 Modify Parameter 공격 구간의 네트워크–공정 시계열 비교



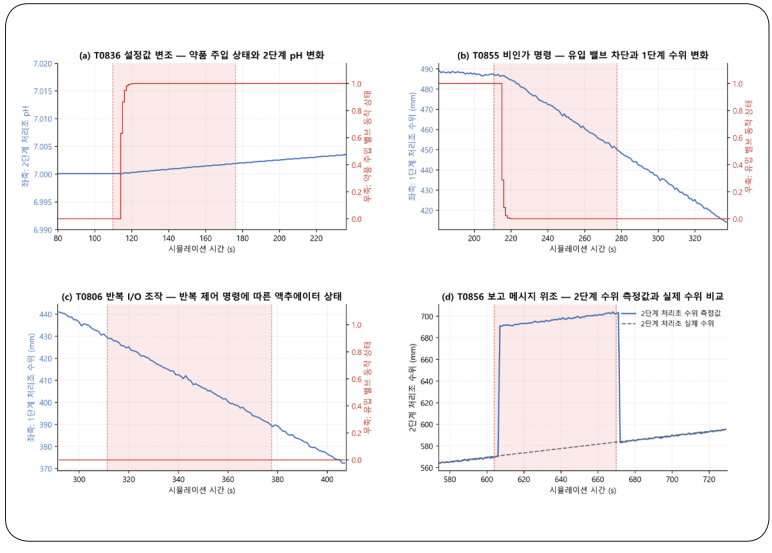
3. 공격 시나리오별 공정 영향

공격 시나리오별 공정 영향은 〈그림 5〉와 〈표 15〉를 중심으로 분석하였다. 〈그림 5〉는 주요 공정 변수의 시간적 변화를, 〈표 15〉는 공격별 관측 대상과 공정 영향을 요약한 것이다. 쓰기 기반 공격군은 네트워크상의 비정상 쓰기 요청이 공정 상태 변화로 연결되는 유형이다. Modify Parameter는 설정값 변경에 따른 pH 관련 변수 변화로, Unauthorized Command Message와 Brute Force I/O는 액추에이터 조작에 따른 수위 또는 유량 변동으로 관측되었다.

〈표 15〉 공격 시나리오별 공정 영향 요약

공격 유형	주요 관측 대상	공정 영향
Modify Parameter	pH 측정값, pH 설정값	설정값 변경에 따른 pH 변화 가능
Unauthorized Command Message	유입 밸브 상태 및 Stage 1 처리조 수위	액추에이터 조작에 따른 수위 변화 가능
Brute Force I/O	액추에이터 조작에 따른 수위 변화 가능	반복 조작에 따른 유량 변동 가능
Point & Tag Identification	주요 공정 변수	직접적인 공정 변화 제한
Denial of Service	주요 공정 변수	본 실험 조건에서는 공정 영향 제한
Spoof Reporting Message	실제 상태, 측정 상태	센서 측정값의 인위적 변화
Adversary-in-the-Middle	주요 공정 변수	직접적인 변화가 제한적

〈그림 5〉 공격 구간별 주요 공정 변수 변화



반면 Point & Tag Identification과 Denial of Service는 본 실험 조건에서 직접적인 공정 변수 변화가 제한적이었다. 전자는 주소 영역을 조회하는 정찰 행위이고, 후자는 FC03 요청 폭주로 관측되는 네트워크 부하 공격이므로 공정 로그보다 요청 빈도와 접근 패턴을 중심으로 해석하는 것이 적절하다.

Spoof Reporting Message는 네트워크 기능 코드 변화보다 실제 상태와 측정 상태 간 불일치가 핵심 단서로 나타나므로, 이 공격은 센서 측정값, 실제 공정 상태, 제어 상태 간의 일관성 분석을 통해 식별할 필요가 있다. Adversary-in-the-Middle은 공정 변수 변화가 제한적이며, 주요 단서는 공정 로그보다 ARP 패킷 및 MAC-IP 매핑 변화에서 확인된다.

쓰기 기반 공격은 네트워크 이벤트와 공정 변화가 함께 나타나는 반면, 정찰·서비스 거부·중간자 공격은 주로 네트워크 특성으로 구분된다. 또한 센서 측정값 변조와 같이 네트워크 단서가 제한적인 공격은 공정 상태 로그 분석이 필수적이며, 이는 수처리 OT/ICS 침입 탐지에서 네트워크 트래픽과 공정 상태 데이터를 함께 고려해야 함을 보여준다.

VI. 한계점

본 논문의 실험 결과는 네트워크 트래픽과 공정 상태 로그를 동일 시간축에서 결합할 경우 공격 행위의 의미를 구체적으로 해석할 수 있음을 보여준다. 그러나 본 실험 결과는 제안한 시뮬레이터의 설계 범위와 공격 구현 방식에 따라 해석되어야 하며, 다음과 같은 한계를

가진다.

첫째, 본 시뮬레이터는 실제 수처리 시설의 정밀한 물리·화학 공정을 재현하는 디지털 트윈이 아니라, 침입탐지 데이터셋 생성을 위한 목적 지향형 실험환경이다. 따라서 실제 설비의 배관 구조, 수질 조건, 운영 절차, 안전 계장 시스템을 모두 반영하지는 않는다. 또한 본 연구의 화학 공정 모델은 pH 조정과 자유염소 잔류를 중심으로 구성되었으나, 실제 수처리 공정에서는 다양한 화학적 요인이 pH 및 염소 소모에 영향을 줄 수 있다. 이로 인해 본 연구에서 관측된 공정 변수 변화는 공격 유형별 네트워크-공정 연계 분석의 가능성을 보여주는 결과로 해석되어야 하며, 실제 수처리 시설 전체의 물리적 거동을 일반화한 결과로 보기는 어렵다. 향후 연구에서는 실제 수처리 설비 운전 자료 또는 공개 ICS 데이터셋과 비교 검증을 수행하고, 다중 화학종 모델로 확장할 필요가 있다.

둘째, 본 논문의 공격 구현과 시나리오 구성은 통제된 실험 조건에 한정된다. 본 논문에서 Spoof Reporting Message는 실제 Modbus 응답 패킷을 위조하는 방식이 아니라 센서 측정값에 편차를 부여하는 방식으로 구현하였으며, Adversary-in-the-Middle은 Modbus payload 변조가 아니라 ARP 기반 통신 경로 개입으로 구현하였다. 또한 본 연구는 공격 시나리오별 대표 구간을 중심으로 네트워크 특성과 공정 영향을 분석하였으나, 실제 OT/ICS 공격은 정찰, 설정값 변경, 액추에이터 조작, 통신 경로 개입이 시간적으로 결합된 복합 공격 형태로 발생할 수 있다. 따라서 향후 연구에서는 HMI-PLC 통신 과정에서 센서 응답 또는 제어 명령의 payload가 변조되는 공격을 구현하고, 단일 공격 중심의 시나리오를 복합 공격 시나리오로 확장할 필요가 있다. 나아가 생성 데이터를 기반으로 네트워크 기반 탐지,

공정 기반 탐지, 공정-네트워크 결합 탐지 모델의 성능을 비교할 필요가 있다.

셋째, 본 논문은 수처리 공정을 대상으로 하였기 때문에, 제안한 공격별 관측 특성이 전력, 가스, 교통 등 다른 OT/ICS 환경에서도 동일하게 나타나는지는 확인하지 못하였다. 본 논문에서는 MITRE ATT&CK for ICS를 참고하여 공격 시나리오를 설계하였으나, 이는 공격 유형을 체계적으로 구성하기 위한 기준이며, 동일한 기법에 기반한 공격이라도 적용 환경에 따라 관측 양상은 달라질 수 있다. 실제 OT/ICS 운영 환경은 시설의 목적과 구조에 따라 네트워크 구성, 장비 종류, 통신 주기, 제어 로직, 운영 정책이 서로 다르므로, 동일한 공격이라도 네트워크 특성이나 공정 영향이 다르게 나타날 수 있다. 또한 본 논문의 문헌 조사와 비교 분석은 수처리 테스트베드 및 데이터셋을 중심으로 수행되었으므로, ICS 전반의 시뮬레이터와 침입탐지 데이터셋 연구를 충분히 포괄하지는 못하였다. 향후 연구에서는 본 시뮬레이터의 계층 분리 구조와 위협 모델을 수처리 이외의 OT/ICS 도메인으로 확장할 필요가 있다. 아울러 전력, 가스, 교통 등 다양한 ICS 분야의 시뮬레이터 및 침입탐지 데이터셋 연구를 함께 검토하고, 도메인별 공정 변수, 제어 로직, 안전 요건의 차이를 반영한 공격 시나리오와 관측 지점을 도출할 필요가 있다.

Ⅶ. 결론 및 향후 연구

본 논문은 수처리 OT/ICS 환경에서 침입탐지 데이터셋 생성을 위한 사이버보안 실험용 시뮬레이터를 설계하고 구현하였다. 제안한

시뮬레이터는 수처리 공정, PLC, HMI, 공격자 노드, Modbus/TCP 기반 제어 네트워크를 결합하여 정상 운전과 공격 상황을 동일한 실험 조건에서 반복 생성할 수 있도록 구성하였다. 또한 네트워크 트래픽, 공정 상태 로그, 공격 라벨, 실험 설정 정보를 함께 수집함으로써, 공격 행위와 공정 상태 변화의 관계를 동일 시간축에서 분석할 수 있는 데이터 생성 구조를 제시하였다.

본 논문의 주요 의의는 기존 공개 데이터셋의 고정된 공격 시나리오와 수집 조건의 한계를 보완하여, 연구자가 통신 주체, 기능 코드, 접근 주소, 요청 주기, 공격 지속시간, 공격 대상 등을 조정하며 반복 실험을 수행할 수 있는 환경을 제안했다는 점에 있다. 특히 생성된 데이터셋은 PCAP 기반 네트워크 트래픽과 CSV 기반 공정 상태 로그를 분리하여 저장하면서도 동일한 실험 시간축에서 연계할 수 있도록 구성하였다. 이를 통해 패킷 단위의 네트워크 분석뿐만 아니라 공정 변수 변화, 액추에이터 상태, 센서 측정값 불일치 등을 함께 고려하는 공정 인지형 침입탐지 연구에 활용될 수 있다.

실험 결과, 정상 운전 구간에서는 FC01·FC03 중심의 주기적 조회 패턴과 FC05 미관측 특성이 나타났다. 공격 구간에서는 쓰기 기반 공격이 FC05·FC06 요청 증가와 공정 변수 변화로, 읽기 및 트래픽 기반 공격이 요청 빈도와 주소 접근 패턴으로 구분되었다. 또한 Spoof Reporting Message는 실제 상태와 측정 상태 간 불일치로, Adversary-in-the-Middle은 ARP 패킷 증가와 MAC-IP 매핑 변화로 관측되었다. 이는 기능 코드나 패킷 수와 같은 단일 네트워크 지표만으로는 공격의 의미를 충분히 해석하기 어렵고, 네트워크 이벤트와 공정 상태 로그를 함께 분석해야 함을 보여준다. 특히 Modify Parameter 공격 구간의 네트워크-공정 시계열 비교에서는 FC06 요청

증가와 pH 관련 변수 변화가 공격 라벨을 기준으로 시간적으로 연결됨을 확인하였다. 이는 생성된 데이터셋이 정상·공격 패킷 구분뿐만 아니라, 공격 요청이 공정 상태 변화로 이어지는 과정을 분석하는 데 활용될 수 있음을 의미한다.

향후 연구에서는 VI장에서 논의한 한계를 보완하기 위해 공개 ICS 데이터셋과의 비교 검증을 수행하고, 실제 Modbus payload 변조 공격과 복합 공격 시나리오를 구현할 필요가 있다. 또한 생성된 데이터를 기반으로 네트워크 기반 탐지, 공정 기반 탐지, 공정-네트워크 결합 탐지 모델의 성능을 비교함으로써, 제안한 데이터셋이 침입탐지 연구에 실질적으로 활용될 수 있는지를 정량적으로 검증할 계획이다. 이를 통해 본 시뮬레이터를 수처리 환경에 특화된 데이터 생성 도구에서 다양한 OT/ICS 침입탐지 연구로 확장 가능한 실험 기반으로 발전시키고자 한다.

〈참고문헌〉

Ahmed, Chuadhry Mujeeb, Venkata Reddy Palleti, and Aditya P. Mathur. 2017. "WADI: A Water Distribution Testbed for Research in the Design of Secure Cyber Physical Systems." In Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks, 25-28. New York: ACM.

Antonioli, Daniele, and Nils Ole Tippenhauer. 2015. "MiniCPS: A Toolkit for Security Research on CPS Networks." In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, 91-100. New York: ACM.

Conti, Mauro, Denis Donadel, and Federico Turrin. 2021. "A Survey on Industrial Control System Testbeds and Datasets for Security Research." IEEE Communications Surveys & Tutorials 23(4): 2248-2294.

Gao, Wei, and Thomas H. Morris. 2014. "On Cyber Attacks and Signature Based Intrusion Detection for Modbus Based Industrial Control Systems." Journal of Digital Forensics, Security and Law 9(1), Article 3.

Goh, Jonathan, Sridhar Adepu, Khurum Nazir Junejo, and Aditya Mathur. 2017. "A Dataset to Support Research in the Design of Secure Water Treatment Systems." In Critical Information Infrastructures Security, edited by G. Havarneanu, R. Setola, H. Nassopoulos, and S. Wolthusen, 88-99. Cham: Springer.

Lin, Qin, Sicco Verwer, Robert Kooij, and Aditya Mathur. 2020. "Using Datasets from Industrial Control Systems for Cyber Security Research and Education." In Critical Information Infrastructures Security, edited by Simin Nadjm-Tehrani, 122-133. Cham: Springer.

Mathur, Aditya P., and Nils Ole Tippenhauer. 2016. "SWaT: A Water Treatment Testbed for Research and Training on ICS Security." In Proceedings of the 2016 International Workshop on Cyber-Physical Systems for Smart Water Networks, 31-36. Vienna: IEEE Computer Society.

Morris, Thomas, Rayford Vaughn, and Yoginder S. Dandass. 2011. "A Testbed for SCADA Control System Cybersecurity Research and Pedagogy." In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Article 27. New York: ACM.

Morris, Thomas, and Wei Gao. 2014. "Industrial Control System Traffic Data Sets for Intrusion Detection Research." In Critical Infrastructure Protection VIII, edited by Jonathan Butts and Sujeet Shenoi, 65-78. Berlin: Springer.

Shin, Hyeok-Ki, Woomyo Lee, Jeong-Han Yun, and HyoungChun Kim. 2020. "HAI 1.0: HIL-Based Augmented ICS Security Dataset." In 13th USENIX Workshop on Cyber Security Experimentation and Test. Berkeley, CA: USENIX Association.

Stouffer, Keith, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, and Michael Thompson. 2023. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology.

Taormina, Riccardo, Stefano Galelli, Nils Ole Tippenhauer, Elad Salomons, Avi Ostfeld, Demetrios G. Eliades, Mohsen Aghashahi, Raanju Sundararajan, Mohsen Pourahmadi, M. Katherine Banks, B. M. Brentan, M. Herrera, Amin Rasekh, Enrique Campbell, I. Montalvo, G. Lima, J. Izquierdo, Kelsey Haddad, Nikolaos Gatsis, Ahmad Taha, Saravanakumar Lakshmanan Somasundaram, D. Ayala-Cabrera, Sarin

E. Chandy, Bruce Campbell, Pratim Biswas, Cynthia S. Lo, D. Manzi, E. Luvizotto Jr., Zachary A. Barker, Marcio Giacomoni, M. Fayzul K. Pasha, M. Ehsan Shafiee, Ahmed A. Abokifa, Mashor Housh, Bijay Kc, and Ziv Ohar. 2018. “The Battle of the Attack Detection Algorithms: Disclosing Cyber Attacks on Water Distribution Networks.” Journal of Water Resources Planning and Management 144(8): 04018048.

Design and Implementation of a Simulator for Intrusion Detection Dataset Generation in Water Treatment OT/ICS

Ann Seok Hyun | Department of AI-Based Convergence, Dankook University
Cho Seong-je | Department of Software Science, Dankook University

This paper presents the design and implementation of a cyber-physical experimental simulator for generating high-fidelity intrusion detection datasets in water treatment OT/ICS environments. Collecting attack data from real-world industrial facilities is severely restricted by process stability, cost constraints, and the risk of operational disruption. To address this, we propose a controlled experimental framework that facilitates the repetitive generation of normal operations and diverse attack scenarios. The proposed simulator integrates a water treatment process model, PLC/HMI control logic, an attacker node, and Modbus/TCP communication protocols to simultaneously capture network traffic, process state logs, and corresponding attack labels. Based on the MITRE ATT&CK for ICS framework, we implemented various attack scenarios, including parameter modification, unauthorized commands, brute force I/O, point and tag identification, denial-of-service (DoS), and adversary-in-the-middle (MitM) attacks. Experimental results demonstrate that attack characteristics differ significantly across network and process layers. Crucially, our findings indicate that several attack types are difficult to detect via packet-level analysis alone, underscoring the necessity of integrated analysis between network traffic and process state variables for robust threat detection.

Keyword Industrial Control System, Operational Technology, Intrusion Detection, Water Treatment Plant, Cyber-Physical Security

* This work was supported by the IITP(Institute of Information & Communications Technology Planning & Evaluation)-ICAN(ICT Challenge and Advanced Network of HRD) grand funded by the Korea government(Ministry of Science and ICT)(IITP-2026-RS-2023-00259867) and This work was supported by the IITP(Institute of Information & Coummunications Technology Planning & Evaluation)-ITRC(Information Technology Research Center) grant funded by the Korea government(Ministry of Science and ICT)(IITP-2026-RS-2023-00259967)