Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.1, Feb. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.1.123

중간자 PLC를 이용한 CPS 은닉형 공격 실험환경 구축 방안

장 엽,†‡ 이 우 묘, 신 혁 기, 김 신 규
ETRI 부설연구소

An Experimental Environment for Simulation of Stealthy Deception Attack in CPS Using PLCitM (PLC in the Middle)

Yeop Chang,†‡ Woomyo Lee, Hyeok-Ki shin, Sinkyu Kim
The Attached Institute of ETRI

요 약

사이버 물리 시스템(CPS: Cyber-Physical System)은 물리시스템과 사이버시스템이 통합되어 운영되는 시스템을 말한다. CPS는 대상 물리시스템을 안정적으로 운영하기 위해 다수의 센서를 이용하여 끊임없이 물리 대상을 모니터링하고 현재 상태에 따라 액추에이터 제어를 수행한다. 만약 악의적인 공격자가 자신들의 공격을 은닉하기 위해서 센서들의 측정값을 대상으로 위변조 공격을 수행한다면, 수집된 데이터에 기반하여 운영되는 사이버시스템은 현재 물리시스템의 운영 현황을 확인할 수 없게 된다. 이는 자동화 시스템 및 운전원의 대응을 지연시켜 더욱 큰 피해가 발생하게 된다. 점차 정교해지는 타겟형 공격들로부터 CPS를 안전하게 보호하기 위해서는 센서 및 측정값을 대상으로 수행되는 은닉형 공격을 탐지할 수 있는 대응기술을 개발해야 한다. 그러나 다양한 이기종 장치들이 존재하는 CPS에서 실제 현장장치들을 대상으로 취약점을 분석하고 실증하는 과정은 많은 시간을 필요로 한다. 따라서 본 연구에서는 CPS 은닉형 공격 탐지 기술의 성능 검증에 활용 가능한 중간자 PLC 실험환경 구축 방안을 제안하고 그 실험결과를 제시한다.

ABSTRACT

Cyber-Physical System (CPS) is a system in which a physical system and a cyber system are strongly integrated. In order to operate the target physical system stably, the CPS constantly monitors the physical system through the sensor and performs control using the actuator according to the current state. If a malicious attacker performs a forgery attack on the measured values of the sensors in order to conceal their attacks, the cyber system operated based on the collected data can not recognize the current operation status of the physical system. This causes the delay of the response of the automation system and the operator, and then more damage will occur. To protect the CPS from increasingly sophisticated and targeted attacks, countermeasures must be developed that can detect stealthy deception attacks. However, in the CPS environment composed of various heterogeneous devices, the process of analyzing and demonstrating the vulnerability to actual field devices requires a lot of time. Therefore, in this study, we propose a method of constructing the experiment environment of the PLCitM (PLC in the middle) which can verify the performance of the techniques to detect the CPS stealthy deception attack and present the experimental results.

Keywords: Cyber Physical System, Stealthy Deception Attack, PLCitM (PLC in the Middle)

Received(09. 26. 2017), Modified(12. 20. 2017), Accepted(12. 20. 2017)

† 주저자, ranivris@nsr.re.kr
‡ 교신저자, ranivris@nsr.re.kr(Corresponding author)

I. 서 론

사이버 물리 시스템(CPS:Cyber-Physical System)은 IT 기반 기술을 활용하여 실제 물리 대상을 제어하는 시스템을 말한다. 발전, 송변전 시스템, 철도운영시스템, 수처리시스템과 같은 사회기반시설만이 아닌 자동차, 지능형 가전기기, 인공 심장박동기 등 주변의 다양한 기기들 모두 넓은 의미로 CPS에 포함된다. 기반시설을 다루는 CPS의 오동작 시에는 대규모 정전이나, 기기의 고장 파괴 등으로 인한 대규모의 경제적/인명 피해가 발생할 수 있어 국가 단위의 조직적인 공격자들의 주요 공격 대상이 되고 있다[9,10]. 이러한 공격자들의 공격으로부터 CPS를 안전하게 보호하기 위해서는 IT 구성요소(서버, 네트워크 어플리케이션 등)를 대상으로 하는 기존의 IT 보안 기술만이 아닌, 센서, 액추에이터, 제어 프로세스 자체 등 CPS의 물리적 특성을 고려한 보안기술의 적용이 필요하다.

CPS는 대상 물리 시스템을 효율적, 안정적으로 운영하기 위해 다수의 센서를 통해 현재 상황을 모니터링하고 측정된 값을 기반으로 액추에이터의 동작을 제어한다. CPS의 정상적인 운영을 위해서는 센서들로부터 수집된 측정값에 대한 신뢰도는 무엇보다도 중요하다. 일반적으로 센서나 액추에이터들은 물리적으로 접근이 어려운 보호된 장소에 설치되어 운영되고 있지만, 지리적으로 분산되어 운영되는 시스템의 경우 공격자들의 접근을 원천적으로 차단하기 어렵다. 공격을 추적할 수 있는 디지털 기록이 남지 않아 타겟형 공격자의 공격 대상이 되고 있다. 타겟형 공격자들은 공격의 피해를 극대화하기 위해 은닉형 공격(Stealthy deception attack)을 선호한다. 은닉형 공격이란 기기를 오동작 시키는 것에서 멈추지 않고 센서 및 측정값을 속여 운영자의 대응을 최대한 지연시켜 물리적 피해를 극대화하는 공격을 말한다. 이러한 CPS 은닉형 공격 기법 및 탐지 기법에 대한 다수의 연구가 진행되고 있다.

센서 및 측정값을 대상으로 하는 은닉형 공격은 사이버적인 방식과 물리적인 방식 모두를 통해 가능하다. 대표적인 물리적 공격 방식은 빛이나 소리와 같이 센서가 측정하는 물리적 현상 자체를 주입하는 유형과 디지털 회로가 안테나로 사용될 수 있는 특성을 이용하여 전자기적 간섭 효과(EMI: Electro-Magnetic Interference)를 사용하여 신호를 주입하는 유형이 존재한다. 최근들어 센서와 같은 현장기기들에 IT 기술이 도입됨에 따라, 전통적인 센서 보안에서는 고려하지 않던 사이버 측면의 공격 가능성도 증가하게 되었다. 대표적인 사이버 공격으로는 센서의 펌웨어 변조, 설정값 변조 등을 통해 센서의 반응치 및 동작 방식을 변경하는 방법 등이 있다. 다양한 경로를 통해 발생할 수 있는 공격을 탐지하기 위해 개별적 측정값 혹은 측정값들의 상관관계를 분석하거나[3,4], 도메인 모델을 활용하여 이상행위를 탐지하는 연구들이 활발히 이뤄지고 있다[1,5,6].

그러나 CPS 센서와 액추에이터의 사이버 및 물리적 취약점이 실제로 존재한다 하더라도 이러한 취약점을 분석하고 실증하는 과정은 높은 수준의 분석 기술과 많은 시간을 요구한다. 다양한 이기종 장치들이 존재하는 CPS에서 현장장치들을 대상으로 일일이 취약점 분석을 수행하는 것은 방어자 입장에서는 매우 비효율적이다. 따라서 연구자들은 CPS 내 존재하는 다양한 공격 중 한 두 유형의 공격을 실증하고, 이를 탐지할 수 있는 방법들을 제시하였다. 하지만 공격자들은 방어자가 실증한 유형 이외에도 다른 경로를 통해 공격을 수행할 수 있다. 탐지 모델이 다양한 유형의 은닉형 공격을 탐지할 수 있는지 실증하기 위해서는 은닉형 공격과 유사한 형태의 공격을 효율적으로 모사할 수 있는 환경이 필요하다.

따라서 본 연구에서는 Fig.1과 같이 센서/액추에이터와 제어 PLC(Programmable Logic Controller) 사이의 신호 전달 구간에서 신호를 마음대로 조작할 수 있는 중간자 PLC(PLCitM)를 설치하여 다양한 은닉형 공격 시나리오를 구현할 수 있는 실험환경 구축방안을 제시한다. 중간자 PLC는 다양한 센서 및 액추에이터의 입출력 신호와 연결이 용이하고, 센서 및 측정값의 위변조 공격에 특화된 복잡한 공격 시나리오를 손쉽게 구현할 수 있다. 테스트베드에 중간자 PLC를 설치하여 CPS 공격 실

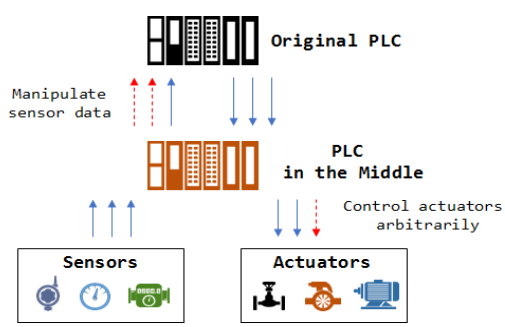

Fig. 1. A Structure of PLCitM

험환경을 구축하고 은닉형 CPS 공격을 수행함으로써 제안한 실험환경 구축방안이 도메인 지식을 활용한 공격자의 공격을 효율적으로 모사해 낼 수 있음을 확인하였다. 따라서 본 논문에서 제안하는 CPS 공격 실험환경 구축방안은 은닉형 공격방안 연구 및 탐지모델의 성능 검증 연구에 활용될 수 있을 것이다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 CPS를 대상으로 하는 은닉형 공격의 사이버적/물리적 공격 기술 및 탐지 기술 현황에 대해 설명하고, 우리 연구가 해결하고자 하는 문제의 범위를 정의한다. Ⅲ장에서는 실험에 사용한 테스트베드 및 구성요소에 대해 설명한다. Ⅳ장에서는 중간자 PLC를 이용한 CPS 공격 실험 환경을 제안하고, Ⅴ장에서는 중간자 PLC 실험 환경을 이용한 CPS 공격 시나리오 실증 및 그 결과에 대해 기술한다. 다음 중간자 PLC 이용한 실험환경 구축방안의 효율성 및 한계점에 대해 정리하고 결론을 맺는다.

Ⅱ. 사이버-물리 시스템 대상 은닉형 공격 및 탐지방안 연구 동향

2.1 은닉형 공격

CPS를 대상으로 하는 은닉형 공격은 사이버적으로 탐지를 피하기 위해 은밀하게 수행되는 공격에서 그치지 않고, 대상 물리시스템의 현재 상황을 속여 피해가 발생한 상황을 숨기는 것을 포함한다. CPS 은닉형 공격은 물리적 특성을 반영한 정교화된 오신호 주입(False data injection) 공격에 속한다.

이런 은닉형 공격은 Fig.2와 같이 CPS 구성요소 및 통신 구간 어디서나 발생할 수 있으며, 개별적 구성요소를 대상으로 혹은 복합적으로 공격이 발생할 수 있다.

센서가 물리적 현상을 디지털 신호로 변환하기 전에 물리적 신호 주입을 통해 공격을 수행하거나(Attack 1), 디지털 신호로 변환 후에 임베디드 기기 및 제어 소프트웨어가 구동되는 서버 혹은 네트워크 단에서 공격이 가능하다(Attack 2~5). 어느 구간에서라도 은닉형 공격이 성공적으로 수행된다면, CPS 시스템에서 물리적 사고가 발생할 수 있다. 대표적인 CPS 공격 사례인 Stuxnet[9]은 PLC의 로직을 변경하고(Attack 4) HMI(Human Machine Interface) 소프트웨어의 통신 DLL을 하이재킹하여(Attack 6), 우라늄 농축 원심분리기의 회전 속도를 속임으로써 운전원의 사고 상황 발생 인지 및 대처를 최대한 지연시켜 이란의 핵 시설에 피해를 발생시킨 바 있다.

이러한 은닉형 공격은 낮은 단계에서 수행될수록 탐지 및 추적이 어려워진다. 특히 센서의 물리적 인터페이스를 대상으로 이루어지는 공격(Attack 1) 공격 발생 시에 디지털 기록이 남지 않고, 디지털 기반 무결성 검증 기술 적용 이전 구간이기 때문에 IT 기반 보안 기술을 활용한 CPS 공격 탐지가 어렵다. 따라서 CPS의 물리적 특성을 고려한 탐지 기술들이 제시되고 있다.

2.2 은닉형 공격 및 방어기술 연구 현황

CPS 은닉형 공격은 CPS 구성요소 어느 곳에서나 발생할 수 있으며, 물리적인 방법과 사이버적인

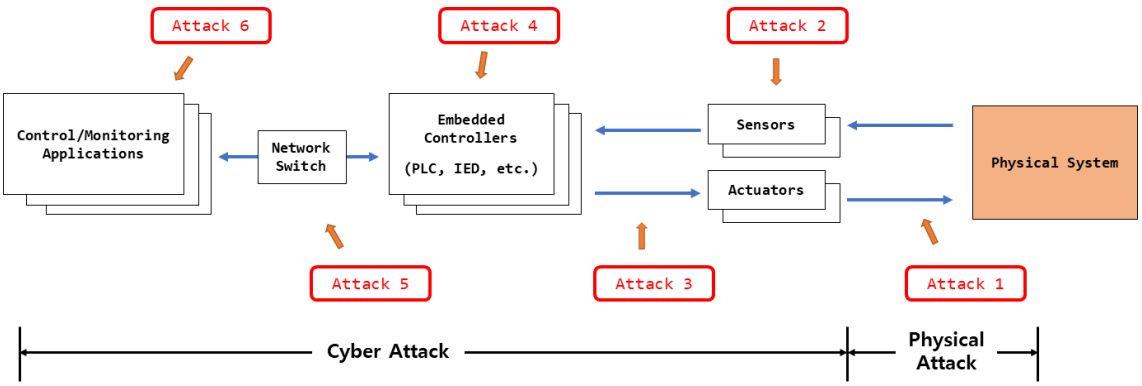

Fig. 2. Attack Surfaces of Stealthy Deception Attack in CPS

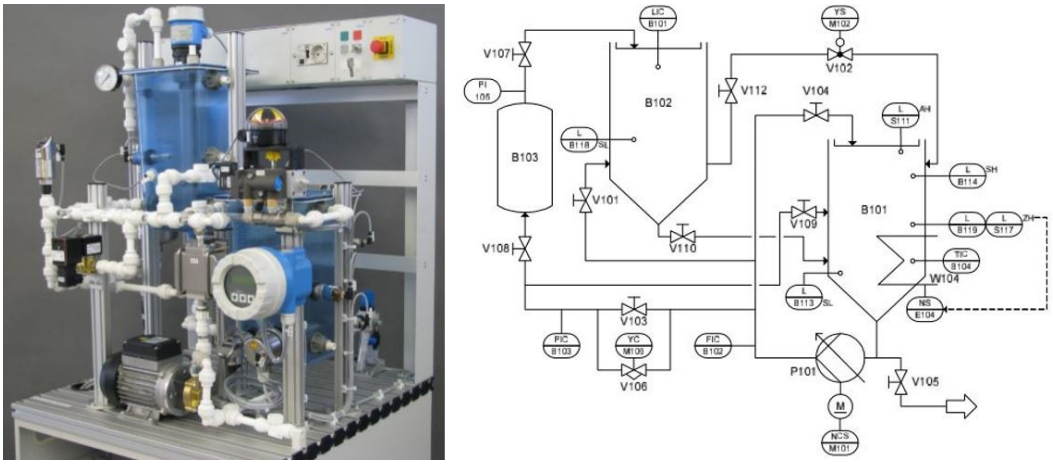

Fig. 3. CPS(Cyber Physical System) Test-bed

방법을 통해 이루어질 수 있다.

물리적인 공격은 센서를 대상으로 물리적인 접촉 없이 수 미터 이상의 거리에서 신호를 주입하는 공격 기법에 초점을 두고 연구가 진행되고 있다. 센서에 신호를 주입하는 방식은 크게 물리적인 신호를 직접 주입하는 방식과 전자기 간섭효과를 이용하는 방식으로 구분된다. 물리적인 신호를 직접 주입하는 위협 사례로는 차량의 Lidar 센서에 인위적으로 강한 빛을 주입하여 차량이 물체를 인식하지 못하도록 하여 충돌이 일어나게 하거나 반대로 물체에서 반사된 것으로 보이는 빛을 주입하여 제동 시스템을 임의로 동작시킬 수 있는 위협이 제시된 바 있다[13]. GPS 정보를 속여 의도하지 않은 방향으로 무인비행체의 경로를 조작할 수 있는[11] 공격 또한 제시된바 있다.

Mo 등[2]은 비교적 쉽게 구축 가능한 안테나 장비를 이용하여 신체 밖에서 인공심작박동기의 오동작을 유발할 수 있으며, 마이크로 폰에 가짜 소리를 주입할 수 있음을 실험적으로 입증하였다. 대부분의 CPS 센서들은 외부의 신호들이 디지털 회로 안으로 주입이 되는 것을 막기 위해서 다양한 전자기 차폐 기술 및 잡음 제거 기술이 도입되어 있다. 이러한 기술들은 주로 해당 장비의 운영환경에서 자연적으로 발생할 수 있는 외부의 신호를 고려하여 설계되었으므로 지능형 공격자의 의도적인 공격을 차단하기에는 부족하다.

의도적인 공격을 막기 위해 시스템 모델과 독립적으로 공격자가 알 수 없는 노이즈를 생성하도록 하여 리플레이 공격을 탐지하는 방안[8]이나 능동형 센서에 시도-응답 인증(Challenge-response authentication) 기술을 적용하여, 신호 발생기가 랜덤하게 유휴 상태로 동작하게 되고 유휴 상태에 있을 때 공격자에 의해 발생된 신호가 탐지될 경우 이를 공격으로 판단하여 오신호 주입 가능성을 최소화하는 방안[7]이 제시된 바 있다.

또한 최근들어 마이크로프로세서가 내장된 스마트 센서가 보급됨에 따라 센서 펌웨어를 대상으로 하는 공격 기법이 소개되었다. Krotofil 등[4]은 센서의 마이크로프로세서용 펌웨어 바이너리 코드를 작성하여, 배관의 밸브를 닫을 경우 발생하는 수격 현상의 데이터를 가상으로 발생시킴과 동시에 운영자가 쉽게 인식하지 못하도록 노이즈를 삽입하고 그 결과를 보였다. 이런 펌웨어 변조 및 설정값 변경 등을 차단하기 위해 연산능력 및 비용 문제로 적용되지 않던 인증서 기반 무결성 검증 기술, 사용자 인증, 탬퍼링 방지 등의 기술이 점차 적용되고 있다.

공격자들의 은닉형 공격을 탐지하기 위해서는 센서로부터 수집된 데이터가 신뢰할 수 있는 값인지 지속적으로 분석해야 한다. 특히 센서의 물리적 인터페이스를 통해 공격이 이루어진 경우, 측정값의 분석 없이 디지털 시스템 단의 보안 기술만을 활용한 탐지는 불가능하다. 공격자의 지능화된 공격을 탐지하기 위해서 측정값을 분석하는 방안에 대한 연구가 활발히 진행되고 있다.

측정값 분석을 통한 인위적인 공격 탐지를 위해서 센서 노이즈의 엔트로피 분석, 센서들 간의 상관관계, 물리적 모델을 활용한 방안들이 제시되었다. Krotofil 등[3]은 공격자들이 인위적으로 노이즈를 삽입한 경우 엔트로피 분석을 통해 이를 탐지하는 방

법과, 반응기(Chemical reactor)의 압력센서와 온도센서와 같이 강한 연관성이 있는 센서들을 묶어 이들의 상관관계를 분석하여 데이터 위변조를 탐지하는 연구를 제시한 바 있다. Amin 등[5,6]은 유체역학 모델기반 고장진단 기법을 적용하여 다음 상태 예측값과 실제 센서 측정값을 비교하여 이상행위를 탐지하는 방안을 제시하였다. 제안한 탐지 방안들은 동시에 다수의 센서들을 대상으로 공격이 발생하지 않는 한 이상행위를 탐지함을 주장하고 있다. 이러한 탐지 기법은 인공위성과 같이 높은 신뢰성을 요구하는 시스템에서 서브시스템의 고장이나 오작동 등의 돌발 상황이 발생하더라도 지속적인 임무수행을 할 수 있도록 고장 검출 및 분리(FDI: Fault Detection and Isolation)가 가능하게 설계하는 방식과 동일하나 의도적인 공격을 탐지할 수 있다는 점에서 차이점이 존재한다.

2.3 마무리

그간 CPS 은닉형 공격 기술 및 탐지 기술 연구는 실제 해당 공격이 가능함을 보이기 위해, 공격을 직접 재연하고 공격을 탐지하는 방법을 제시하였다. 실제 공격을 구현하는 방법은 연구자들의 깊은 배경지식과 많은 시간을 필요로 하며, 제어시스템의 모든 구성 요소들에 대한 공격 및 방어 연구는 현실적으로 불가능하다. 이전의 연구 및 CPS 공격 사례에서 확인된 것처럼 우리는 다양한 공격 벡터를 통해 CPS 센서 및 측정값을 대상으로 한 은닉형 공격이 성공적으로 진행될 수 있음을 인지하고, 다양한 구간에서의 공격을 간편하고 체계적으로 모사해 낼 수 있는 중간자 PLC를 이용한 실험환경을 구축하였다.

Table 1. Level Sensors in the CPS testbed

Sensor	Symbol	Description
Level probe	B101	- Analog level sensor in B102 - Convert the water level to current (4~20mA)
Proximity switch	B113	- Digital level sensor in B101 - Watch the water shortage - Protect the motor pump, P101
	B114	- Digital level sensor in B101 - Watch the water shortage for Initial state
Float switch	S111	- Digital level sensor in B101 - Watch the water overflow
Level switch	B119	- Digital level sensor in B102 - When the water level reaches B119, closed-loop control starts.

III. 테스트베드 소개

CPS 공격 및 탐지 방안 연구에 사용한 테스트베드는 Festo에서 제작한 MPS® PA Compact Workstation을 이용하였다(Fig.3). 해당 테스트베드는 다수의 디지털 장비와 아날로그 장비로 구성되어 있어 신호 레벨에서 실험을 하기 적합하기 때문에 선정되었다. 테스트베드는 '수위제어'와 '수온제어' 두 개의 제어 공정을 제공한다. 수위제어는 하위 물탱크(T101)에서 상위 물탱크(T102)로 물을 올리는 모터펌프(P101), 하위 물탱크로 흐르는 배관을 개폐하는 볼밸브(V102), 수위를 측정할 수 있는 다수의 디지털/아날로그 센서로 구성되어 있으며, 수온제어는 하위 물탱크에 위치한 발열기(E104)와 온도센서(B104)로 구성된다. 전체 CPS 운영을 담당하는 제어 PLC는 Siemens사의 S7-300 PLC가 장착되어 있다. 본 연구에서 중점적으로 다루는 수위제어 공정에서 사용하는 센서와 액추에이터는 Table 1, Table 2와 같다.

수위제어 공정이 시작되면 모터펌프(P101)가 구동되어 하위 물탱크(T101)에서 상위 물탱크(T102)로 물을 공급하다가 수위가 스위치 센서(B119)에 도달하면 폐루프(closed loop) 제어를 시작한다. 폐루프 제어 동안에는 상위 물탱크의 수위를 측정하는 아날로그 수위 센서(B101) 값을 분석하여 모터펌프와 볼밸브(V102) 출력을 조절하여 상위 물탱크의 수위가 설정값(set point)을 유지하도록 제어한

Table 2. Actuators in the CPS testbed

Actuator	Symbol	Description
motor pump	P101	- Installed between B101 and B102 and pump water - Two operation modes ・Digital mode: 1(Full), 0 (Analog) ・Analog mode : Proportional control to output voltage from PLC
ball valve	V102	- Open the valve to allow water flow from B102 to B101

다. 따라서 제어시스템이 정상 동작하는 동안 상위 물탱크의 수위는 설정값과 근접하게 유지된다.

IV. 중간자 PLC 실험환경

4.1 중간자 PLC 구조

PLC는 다수의 센서들로부터 상태값을 입력받아 현재 상태를 판단하고, 액추에이터에 제어신호를 출력한다. 따라서 센서와 액추에이터를 대상으로 은닉형 공격을 효율적으로 모사하기 위해서 중간자 PLC는 Fig.4와 같이 제어 PLC와 센서/액추에이터 사이에 위치한다. 센서 신호는 중간자 PLC의 입력 모듈에 연결되고, 중간자 PLC의 출력모듈을 통해 제어 PLC의 입력 모듈로 연결된다. 마찬가지로 제어 PLC의 출력 모듈을 통해 나오는 제어신호는 중간자 PLC를 거쳐 액추에이터로 전달된다.

중간자 PLC가 정상모드로 동작하는 경우 입력되는 모든 신호는 조작되지 않고 그대로 전달된다. 공격모드로 동작하는 경우에는 중간자 PLC에 저장된 공격 로직에 따라 센서 신호 또는 PLC 제어출력을 변조하여 액추에이터를 불법 제어한다. 공격모드의 시작은 CPS가 정해진 조건에 다다를 경우 실행되거나 공격자의 공격 시작용 트리거 비트 설정 등을 통해 이뤄진다.

4.2 중간자 PLC 구조를 이용한 공격 모사

다수의 센서와 액추에이터로 구성된 CPS에서 물리적 피해를 야기할 수 있는 공격의 유형은 Table 3.과 같이 크게 3가지(액추에이터 불법제어, 센서 데이터 조작, 은닉형 공격)으로 구분할 수 있다.

액추에이터 불법 제어 공격은, 직접적으로 액추에

Table 3. Category of CPS Attacks Causing Physical Damages

Category	Description
1. Illegal Control of Actuators	Attackers control actuators arbitrarily
2. Manipulation of Sensor Data	Attackers manipulate sensor data to cause undesirable control actions
3. Stealthy Deception Attack	Attackers control actuators arbitrarily and manipulate sensor data to hide attacks

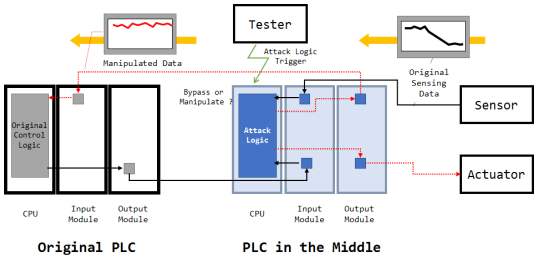

Fig. 4. PLCitM Wiring and How it works

이터 제어를 통해 CPS 오동작을 유발하는 공격이다. 이 공격은 제어시스템이 운전원의 예상과 다르게 동작하기 때문에 탐지 및 빠른 대처가 가능하다. 따라서 공격자들은 CPS에 더 큰 피해를 유발하기 위해서는 보다 정교한 유형의 공격을 수행해야 한다. 센서 데이터 조작 공격은 측정값을 변조함으로써 제어시스템의 제어를 유도해 내는 유형의 공격이며, 은닉형 공격은 불법 제어와 측정값 위조를 통한 공격 은닉이 함께 발생하는 유형으로 임의의 시점에 공격을 수행할 수 있으며 공격 자체를 운전원이 인지할 수 없기 때문에 제일 큰 피해를 유발할 수 있다.

은닉형 공격의 공격 모사 시에 중간자 PLC는 운전원을 속이기 위해서 정상 상태로 보이도록 측정값을 위조해야 한다. Fig.5는 중간자 PLC가 은닉형 공격을 성공적으로 모사하기 위해 수행해야 하는 작업을 보여준다. (a)와 같이 센서의 측정값이 폐루프 상태에서 주기적인 패턴을 가지는 경우, 시스템의 물리적 특성을 고려하지 않고 (b)와 같이 공격자가 공격 시점의 값을 지속적으로 생성한다면 이는 운전원에 의해 빠르게 대응이 가능하다. 물리적 특성을 고려하여 (c)와 같이 측정값을 생성하는 경우에도 아날로그 센서에서 발견되는 노이즈를 고려하지 않을 경우 운전원이 이상 유무를 빠르게 인식할 수 있다. 따라서 노이즈 패턴까

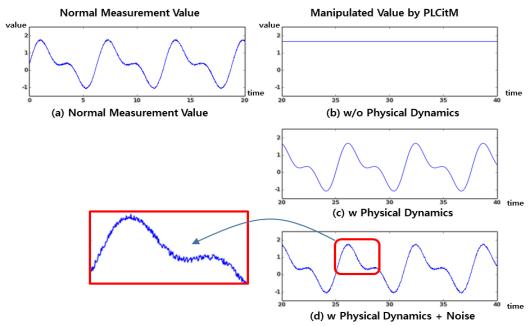

Fig. 5. Sensing Data Manipulation in PLCitM

지 반영하여 (d)와 같이 측정값을 생성할 수 있어야 은닉형 공격을 수행한다고 볼 수 있다. 따라서 중간자 PLC를 이용한 CPS 은닉형 공격을 모사하기 위해서는 대상 CPS의 동작방식에 대한 분석과 함께 노이즈를 고려하여 대상 CPS의 측정값을 유사하게 생성해 낼 수 있어야 한다. 보다 정교한 은닉형 공격을 위해서는 CPS의 제어공정 프로세스의 물리적 특성과 각각의 장치들의 사양에 대한 지식이 필요하다.

V. 중간자 PLC를 활용한 은닉형 공격 실험

본 실험에서는 테스트베드의 수위 제어 공정을 대상으로 중간자 PLC를 이용하여 은닉형 공격을 수행하고 그 결과에 대해 논의한다. 중간자 PLC로는 Siemens 사의 S7-1500을 사용하였으며 PLC 표준 프로그래밍 언어인 FBD(Function Block Diagram)와 STL(STatement List)을 이용하여 중간자 제어로직을 구현하였다.

5.1 은닉형 공격 시나리오 설계 및 구현

은닉형 공격이 성공하기 위해서는 CPS에 물리적 피해가 발생하고 있음에도 불구하고, 이를 운전원이 인식하지 못하게 해야 한다. 따라서 중간자 PLC가 모터펌프 혹은 볼밸브와 같은 액추에이터를 제어함과 동시에 정상 상태로 보이도록 모니터링에 활용되는 수위 센서의 신호를 조작하여 제어 PLC로 전송해야 한다.

Fig.6은 중간자 PLC의 은닉형 공격과 연관된 제어로직의 핵심 코드를 나타내고 있다. Main 블록〔OB1〕은 PLC의 매 주기마다 호출되는 블록으로, 매 스캔주기마다 공격 트리거 비트(Attack_Trigger_bit)가 설정되었는지 체크한다. 공격 트리거 비트 설정값에 따라 다음과 같이 동작한다.

- 공격 트리거 비트가 0일 때 : 정상운영모드로 동작하며 Pump_Level_Bypass〔FC1〕 함수를 호출
- 공격 트리거 비트가 1일 때 : 공격모드로 동작하며 Attck_Pump_Level〔FC10〕 함수를 호출

FC1 함수는 상위물탱크에 설치된 아날로그 수위 센서의 측정값을 입력받아 제어 PLC에 그대로 전달하고, 제어 PLC로부터 펌프 제어명령을 입력받아 펌프에 그대로 전달하는 bypass 함수이다.

공격자가 공격 트리거 비트를 설정하면 OB1 함수는 FC10 함수를 호출하게 되며, FC10 함수는 다음 두 가지 기능을 수행한다.

- 모터펌프를 강제 구동하여 B102의 수위 상승
- Level_Signal_Generator〔FB1〕 함수를 호출하여 은닉용 수위 센서값을 생성하여 제어 PLC에 전달

제어 PLC는 페루프 이전에는 디지털 제어를 통해 모터펌프를 제어하고, 페루프가 시작되면 0~27648 사이의 값으로 아날로그 제어를 수행한다. 모터제어기는 모터펌프 앞단에 설치되어 PLC의 아날로그 출력을 0~10V 전압값으로 변경하여 모터펌프를 제어한다. 이 때 아날로그 모터펌프 제어신호의 최대값은 디지털 모터펌프 제어신호와 거의 유사한 값을 가지므로 실험에서 공격이 트리거되면 모터펌프를 디지털모드로 변환하고 모터펌프 제어신호로 '1'의 값을 출력하여 최대한 빠르게 수위를 높이고자 하였다. 계속 펌프를 강제로 구동시킬 경우 물탱크 용량을 넘어서 상위 물탱크에서 물이 넘치게 된다. 또한 하위 물탱크에 물이 부족할 경우에는 물이 없는 상태에서 모터펌프가 강제로 구동되어 모터의 손상이 발생하게 된다.

운전자가 수위변화를 모니터링하고 있더라도 이러한 공격 상황을 인지하지 못하도록, 중간자 PLC는 은닉용 수위 센서값을 생성하여 제어 PLC에 전달한다. FB1 함수는 구형파와 삼각파 신호에 랜덤값으로 생성한 노이즈 신호를 더하여 수위 측정값을 생성한다. 이 때 실제 센서에서 발생하는 노이즈와 유사하게 보이도록 적절한 배율을 적용하였다. FB1 함수 구현 시에 sine 함수와 rand 함수는 Siemens가 제공하는 공용 라이브러리(Library of General Functions)〔12〕를 활용하였다.

5.2 공격 실험결과

테스트베드에 은닉형 공격 실험을 수행한 결과 모터펌프 제어신호와 수위 센서값의 변화는 Fig.7과 같다. 상위 두 개 그래프는 중간자 PLC에서 모터펌프로 전송하는 제어신호이다. 정상모드에서는 제어 PLC에서 전송된 제어신호가 중간자 PLC를 거쳐 실제 액추에이터로 그대로 전달되지만 공격이 시작되면 중간자 PLC가 모터펌프를 아날로그 모드에서 디지털 모드로 변경하고 모터를 강제 구동시키는 제어

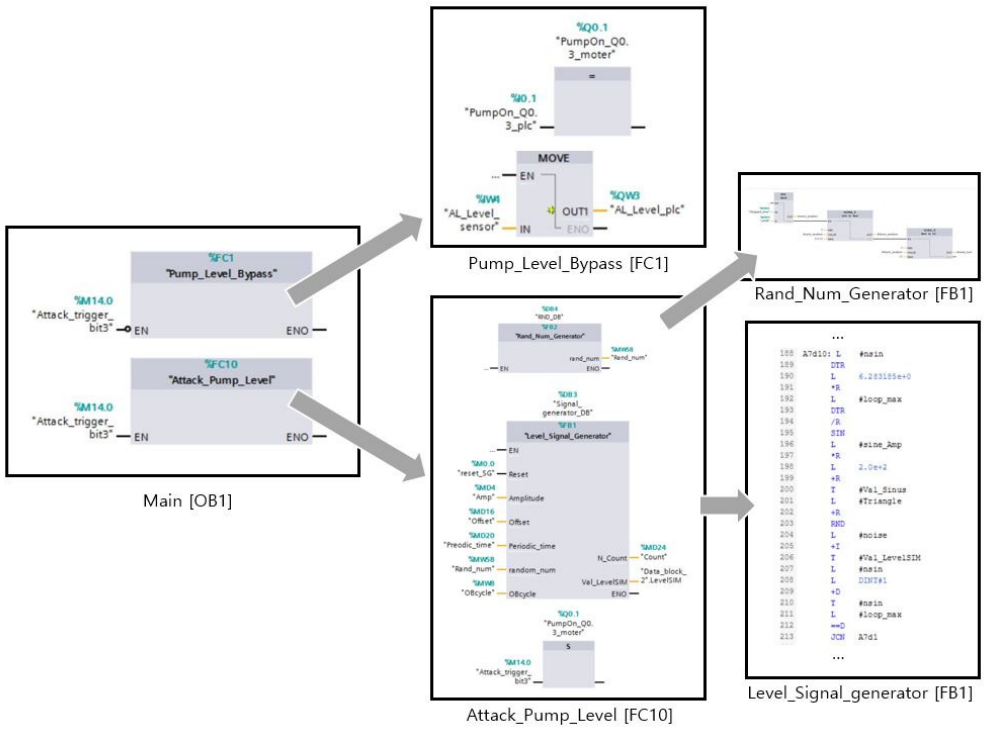

Fig. 6. Control Logic Outline of PLCitM

명령을 전송하므로 아날로그 제어명령값은 '0'이 되고 디지털 제어명령값은 '1'의 값을 가진다. 모터펌프에는 제어 PLC에서 전송하는 제어명령 대신 중간자 PLC가 생성한 제어명령이 전송되므로 모터펌프가 최대출력으로 강제구동되어 물탱크의 수위가 빠르게 상승한다.

Fig.7의 마지막 그래프는 중간자 PLC로 입력되는 아날로그 수위 센서값과 중간자 PLC가 제어 PLC로 전송하는 조작된 아날로그 수위 센서값이다.

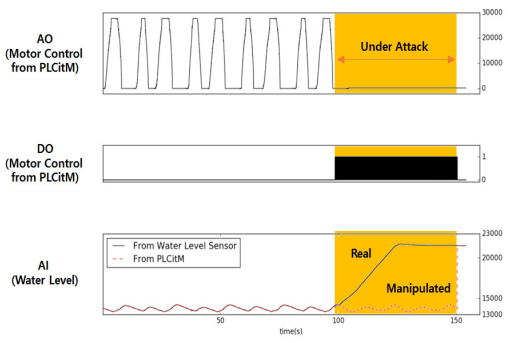

Fig. 7. Attack Experiment Result

이 때 중간자 PLC에 입력되는 신호는 실제 상위 물탱크(B102)의 수위정보이고 중간자 PLC에서 출력되는 신호는 운전원에게 전달되는 조작된 수위모니터링 정보를 의미한다.

중간자 PLC는 정상모드에서 아날로그 수위 센서(LIC/B101)로부터 받은 수위 센서값을 제어 PLC에 그대로 전달하므로 실제 아날로그 수위 센서값과 중간자 PLC에서 출력하는 수위 센서값이 동일하다. 이후 공격트리거비트가 활성화되어 공격모드가 시작되면 중간자 PLC가 모터펌프를 강제 구동시켜 수위가 계속 증가하므로 중간자 PLC로 입력되는 아날로그 수위 센서값이 증가하고 일정시간 이후에는 하위 물탱크에 물이 부족하여 강제로 모터를 구동시킴에도 불구하고 상위물탱크에 수위가 일정하게 유지된다. 공격이 시작되면 중간자 PLC는 공격발생 여부를 은닉하기 위해 정상상태의 수위 센서값과 유사한 신호를 생성하여 제어 PLC에 전송하므로 물탱크의 수위가 상승함에도 불구하고 운전원이 이를 인지할 수 없게 된다.

이와 같이 중간자 PLC를 이용하면 은닉형 공격을 구현하는데 용이하며 공격탐지 연구에 활용 가능

한 데이터를 효율적으로 수집할 수 있음을 확인하였다.

VI. 중간자 PLC 환경을 이용한 실험 평가

6.1 구축 및 구현의 용이성

중간자 PLC를 이용한 실험 환경은 크게 4가지 장점을 갖는다.

첫째, 중간자 PLC는 로직구현 및 자동화가 용이하다. PLC는 프로그래밍 가능한 제어기기로, 실제 제어 PLC와 동일한 프로그래밍 환경을 공유하여 공격 대상 PLC의 제어로직을 바탕으로 공격 시나리오 구현을 손쉽게 할 수 있다. 아울러, 반복적인 작업을 자동화 해줄 수 있어 I/O 퍼징과 같은 검증 평가에 용이하다.

둘째, PLC는 강한 실시간성(Hard real-time)을 제공하여 예측 가능한 타이밍으로 정교한 신호 조작이 가능하다. PLC는 입력조건에 따른 제어출력을 제한된 시간 내에 출력하도록 설계되어 있다. 따라서 입력 조건에 대한 출력 타이밍을 보다 정밀하게 제어할 수 있으며, 이러한 동작 특성을 이용하여 공격 타이밍을 정교하게 제어할 수 있다.

셋째, PLC는 높은 수준의 신호간섭에 노출되는 산업 환경에 적합하도록 설계되어 안정적인 신호 조작이 가능하다. 실제 산업 환경에서 중간자 PLC는 안정적인 리피터의 역할을 하면서 노이즈 추가를 통해 SNR(Signal-Noise-Ratio)을 조절 할 수 있어 정교한 신호 주입이 가능하다. 라즈베리파이와 같은 일반적인 임베디드 보드는 신호간섭에 취약하여 의도치 않은 신호들이 유입될 수 있다.

넷째, PLC는 다양한 신호 모듈(디지털/아날로그 입출력, 타이머, 카운터 등)의 구성을 변경 할 수 있어 각기 다른 신호 형태와 레벨를 갖는 다수의 기기 조작에 용이하다. 다양한 레벨의 전압(0~48VDC, 0~240VAC)과 전류(20mA~40mA)를 사용하는 산업용 센서에 대해서 하나의 중간자 PLC만으로 동시에 다수의 기기들을 모니터링하거나 신호를 조작할 수 있다.

6.2 성능 분석

은닉형 공격 탐지 모델의 경우, 다음 상태를 예측하여 이상 행위 탐지 여부를 수행하기 때문에, 중간자 PLC를 통해 측정값, 제어명령 등이 전달되는 과정에서 지연이 발생할 경우 이러한 탐지 모델의 성능을 저하시킬 수 있다.

중간자 PLC의 최대 스캔 주기를 성능 지연 시간으로 간주하고 중간자 PLC의 개입으로 인한 신호 지연을 확인한 결과, 중간자 PLC의 최대 주기 실행 시간은 3ms를 초과하지 않는 것을 확인할 수 있었다.

우리는 수 ms 이내의 지연이 제어에 큰 영향을 받을 수 있는 특정 분야(예: 고속모션제어 등)를 제외하고 중간자 PLC가 효과적으로 신호를 변경하고 전달할 수 있음을 확인하였다.

6.3 한계점

중간자 PLC를 이용한 구조는, 많은 I/O의 재결선 작업이 필요하며, 아두이노, 라즈베리 파이 등 소형 임베디드 시스템 대비 장비가 고가라는 단점이 있다. 하지만 입출력 신호를 직접적으로 조작할 수 있어 센서의 취약점을 이용하여 실제 공격을 수행하는 과정 보다 시간을 절약할 수 있다. 또한 산업현장에서 사용하는 다양한 유형의 신호를 생성하기에 적합하다.

모든 입출력 신호를 대상으로 은닉형 공격을 수행할 경우, 중간자 PLC는 제어 PLC 두 배에 해당하는 입출력 모듈과 추가적인 결선 작업이 필요하게 된다. 따라서 하드웨어의 구매 비용 하드웨어 장착에 필요한 공간 또한 증가하게 된다. 이러한 문제점은 PLC에 연결된 센서 및 액추에이터 중 중요하거나 공격 가능성이 높은 일부의 장치에만 선택적으로 적용함으로써 극복할 수 있다.

VII. 결론 및 향후 연구

CPS를 대상으로 하는 공격은 사이버적 공격과 함께, 물리적 피해를 최대화하기 위해 CPS의 물리적 특성까지 반영한 고도화된 은닉형 공격으로 진행되고 있다. 따라서 기존의 사이버 보안기술과 함께, CPS 대상 물리 시스템의 특성을 고려하여 공격자의 은닉형 공격을 탐지하는 연구가 반드시 필요하다.

기존의 제어분야에서는 제어시스템의 오동작을 감시하고 탐지하기 위해 고장인지, 고장감내, 안전기반 설계와 같은 메커니즘이 적용되어 있으며, 이러한 메커니즘을 우회하기 위해 공격자들은 더욱 정교한 공

격을 수행하게 된다. 이를 탐지하기 위해서는 방어자 역시 정교한 공격을 모사하고 이를 탐지할 수 있는 기술을 개발해야 한다.

본 연구에서 우리는 지능형 공격자의 은닉형 공격을 모사하고, 탐지 연구에 활용할 수 있는 중간자 PLC 환경을 구축하고, 수위제어기능을 대상으로 은닉형 공격을 모사하였다. 은닉형 공격은 탐지가 어렵기 때문에 공격 과정에서 발생하는 데이터의 실제 수집은 매우 어려우며 운영기관에서는 내부의 중요 정보가 노출될 수 있기 때문에 공개 또한 기피하게 된다. 중간자 PLC를 이용하면 효과적으로 다양한 은닉형 공격에 대해 데이터를 수집할 수 있으며, 수집된 데이터들은 탐지 모델의 실증에 효과적으로 활용될 수 있을 것으로 예상된다. 향후 중간자 PLC 실험환경을 활용하여 보다 정교한 형태의 은닉형 공격 모사와 함께 다양한 형태의 CPS에서 은닉형 공격 탐지 모델의 성능을 검증하는 데 활용할 계획이다.

References

[1] C.M. Ahmed, C. Murguia, and J Ruths. "Model-based Attack Detection Scheme for Smart Water Distribution Networks," Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, pp. 101-113, Apr. 2017

[2] D.F. Kune, J. Backesy, S.S. Clarkz, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu. "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors," IEEE Symposium on Security and Privacy, pp. 145-159, May 2013.

[3] M. Krotofil, J. Larsen, and D. Gollmann. "The Process Matters: Ensuring Data Veracity in Cyber-Physical Systems," Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. pp. 133-144, Apr. 2015.

[4] M. Krotofil, A. Cárdenas, J. Larsen, and D. Gollmann, "Vulnerabilities of cyber-physical systems to stale data-Determining the optimal time to launch attacks," International journal of critical infrastructure protection, vol. 7, no. 4, pp. 213-232, Dec. 2014.

[5] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber Security of Water SCADA Systems-Part I: Analysis and Experimentation of Stealthy Deception Attacks", IEEE Transactions on Control Systems Technology, vol. 21, no. 5, pp. 1963-1970, Sep. 2013.

[6] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber Security of Water SCADA Systems-Part II: Attack Detection Using Enhanced Hydrodynamic Model," IEEE Transactions on Control Systems Technology, vol. 21, no. 5, pp. 1679-1693, Sep. 2013.

[7] Y. Shoukry, P. Martin, Y. Yona, S Diggavi, and M Srivastava. "PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks," Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. pp. 1004-1015, Oct. 2015.

[8] Y Mo, S. Weerakkody, and B. Sinopoli. "Physical Authentication of Control Systems: Designing Watermarked Control Inputs to Detect Counterfeit Sensor Outputs," IEEE Control Systems. vol. 35, no. 1, pp. 93-109, Feb. 2015.

[9] N Falliere, L.O. Murchu, and E. Chien. "W32.Stuxnet Dossier" v1.4, Symantec Security Response, Feb. 2011.

[10] R.M. Lee, M.J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid", SANS ICS Defense Use Cases, Mar.

2016.
〔11〕 C. Kwon, W. Liu, and I. Hwang, "Security Analysis for Cyber-Physical Systems against Stealthy Deception Attacks", 2013 American Control Conference (ACC), Jun. 2013
〔12〕 Library of General Functions (LGF) for S7-1200/1500, https://support.industry.siemens.com/cs/document/109479728/library-of-general-functions-(lgf)-for-step-7-(tia-portal)-and-s7-1200-s7-1500?dti=0&lc=en-US
〔13〕 I. Ruchkum, A. Rao, D.D. Niz, S. Chaki, and D. Garlan, "Eliminating Inter-Domain Vulnerabilities in Cyber-Physical Systems: An Analysis Contracts Approach", Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, pp. 11-22, Oct. 2015

〈저자소개〉

사 진

장 엽 (Yeop Chang) 정회원
2005년 2월: 고려대학교 컴퓨터학과 졸업
2007년 2월: 포항공과대학교 컴퓨터공학과 석사
2007년 1월~2010년 2월: LS산전 주임연구원
2010 ~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 정보보호, 제어시스템 보안, 소프트웨어 공학

사 진

이 우 묘 (Woomyo Lee) 정회원
2010년 2월: 경북대학교 전자전기컴퓨터학부 졸업
2012년 2월: 포항공과대학교 전자공학과 석사
2011년 12월~현재: ETRI 부설연구소 연구원
〈관심분야〉 정보보호, 제어시스템 보안

사 진

신 혁 기 (Hyeok-ki Shin) 정회원
2004년 2월: 경북대학교 전자전기공학부 졸업
2006년 2월: 한국과학기술원 전기및전자공학과 석사
2014년 8월: 한국과학기술원 전기및전자공학과 박사
2014년 9월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 CPS 보안, 로봇공학, 전자공학

사 진

김 신 규 (SinKyu Kim) 정회원
2000년 2월: 연세대학교 기계전자공학부 졸업
2002년 2월: 연세대학교 컴퓨터산업시스템공학과 석사
2014년 2월: 연세대학교 컴퓨터산업시스템공학과 박사
2003년 12월~현재: ETRI 부설연구소 실장
〈관심분야〉 제어시스템, 제어기기, 이상행위 탐지