Journal of the Korea Academia-Industrial cooperation Society
Vol. 19, No. 4 pp. 47-56, 2018

https://doi.org/10.5762/KAIS.2018.19.4.47
ISSN 1975-4701 / eISSN 2288-4688

산업 제어 시스템 보안을 위한 패킷 분석 기반 비정상행위 탐지 시스템 구현

김현석, 박동규*
순천향대학교 정보통신공학과

Implementation of abnormal behavior detection system based packet analysis for industrial control system security

Hyun-Seok Kim, Dong-Gue Park*
Department of Information and Communication Engineering, Soonchunhyang University

요 약 가스, 전력, 수처리, 원자력, 교통 관제 시스템 등과 같은 국가적 규모의 산업 제어 시스템은 점차 발전하는 정보통신 기술에 따라 점차 개방된 네트워크와 공개된 표준 프로토콜을 사용하고 있다. 개방된 네트워크와 공개된 표준 프로토콜을 사용하고 있기 때문에 사이버 공격에 대한 빈도는 점점 증가하고 있는 추세이지만 이에 관련한 후속조치는 매우 부족한 실정이다. 따라서 산업 제어 시스템을 위한 보안 솔루션의 적용은 매우 중요하다. 하지만 실제의 시스템에 보안 솔루션을 적용하는 것은 산업 제어 시스템의 특성 때문에 사실상 불가능하고 기존 시스템에 영향을 주지 않고 공격의 발생 유무를 탐지할 수 있는 보안 시스템이 필수적이다. 따라서 본 논문에서는 산업 제어 시스템에 영향을 주지 않고 비정상행위를 탐지하는 패킷 분석 기반의 침입 탐지 시스템을 제안하고 제안한 침입 탐지 시스템을 실제의 환경을 재현한 산업 제어 시스템 테스트 베드에 적용함으로써 신뢰성 있는 데이터를 기반으로 제안한 시스템의 효율성을 검증한다.

Abstract National-scale industrial control systems for gas, electric power, water processing, nuclear power, and traffic control systems increasingly use open networks and open standards protocols based on advanced information and communications technologies. The frequency of cyberattacks increases steadily because of the use of open networks and open standards protocols, but follow-up actions are limited. Therefore, the application of security solutions to an industrial control system is very important. However, it is not possible to apply security solutions to a real system because of the characteristics of industrial control systems. And a security system that can detect attacks without affecting the existing system is imperative. Therefore, in this paper, we propose an intrusion detection system based on packet analysis that can detect anomalous behaviors without affecting the industrial control system, and we verify the effectiveness of the proposed intrusion detection system by applying it in a test bed simulating a real environment.

Keywords : abnormal behavior detect, cyber attack experiment, industrial control system, intrusion dectection system, ICS security

1. 서 론

산업 제어 시스템(Industrial Control System)은 가스, 전력, 원자력, 교통 등과 같은 국가적 규모의 주요기반시설 및 산업 분야에서 원거리에 산재된 시스템을 감시하고 제어하는 시스템을 통칭한다. 산업 제어 시스템은 과거의 폐쇄적인 네트워크 및 독자적인 프로토콜을 사용하여 사이버 공격으로부터 비교적 안전하였지만, 현대의

본 논문은 순천향대학교 연구비로 연구되었음.
*Corresponding Author : Dong-Gue Park(Soonchunhyang Univ.)
Tel: +82-41-530-1347 email: dgpark@sch.ac.kr
Received January 9, 2018 Revised (1st February 6, 2018, 2nd March 7, 2018, 3rd April 5, 2018)
Accepted April 6, 2018 Published April 30, 2018

산업 제어 시스템은 정보 통신 기술의 진화에 따라 많은 비용절감, 효율성, 편리성, 유연성과 같은 많은 이점이 존재하기 때문에 외부의 개방된 네트워크에 연결하고 공개된 표준 프로토콜을 사용하도록 진화하였다. 따라서 현대의 산업 제어 시스템은 개방된 네트워크에 노출되어 있고 공개된 표준 프로토콜을 사용하기 때문에 많은 공격자로부터 사이버 공격의 대상이 되고 있다. 산업 제어 시스템은 사이버 공격의 정도에 따라 금전적인 손실부터 인간의 생명까지 위협할 수 있기 때문에 산업 제어 시스템을 보호하는 것은 매우 중요한 문제이다. 하지만 대부분의 산업 제어 시스템은 노후화된 하드웨어 및 운영체제를 사용하고 있고 시스템 운영자들의 산업 제어 시스템 보안에 대한 지식 부족 및 관심의 부족으로 인해 많은 취약점이 발견됨에도 불구하고 패치가 이루어지지 않는 등의 문제점이 많이 발생하고 있다[1].

특히 2010년도에 발생한 스턱스넷(Stuxnet) 악성코드 공격은 기존의 IT 시스템에는 전혀 영향을 주지 않지만 산업 제어 시스템에는 치명적인 결과를 초래할 수 있다. 이 공격으로 인해 이란의 원전 시설이 파괴되었다. 이와 같은 사이버 공격을 탐지하기 위하여 산업 제어 시스템에는 기존의 시스템에 영향을 주지 않는 특징을 가진 침입 탐지 시스템(Intrusion Detection System)이 적용되어 비정상행위를 탐지한다. 하지만 대부분의 침입 탐지 시스템은 스턱스 넷과 같이 물리 프로세서의 직접적인 비정상행위는 탐지하지 않는다. 따라서 많은 보안을 위한 연구가 진행되고 있지만 계속해서 발생하는 새로운 방식의 공격에는 대응하지 못하고 있는 실정이다. 따라서 본 논문에서는 스턱스넷과 같은 공격 방식을 탐지하기 위하여 물리 계층과 통신하는 PLC 사이의 구간을 검사 포인트(Check point)로 설정하고 그 구간의 비정상행위를 탐지하는 침입 탐지 시스템을 제안 및 구현하고 기존의 산업 제어 시스템 테스트베드에 적용함으로써 제안한 시스템의 효율성을 검증한다.

본 논문의 구성을 다음과 같다. 2장은 산업 제어 시스템의 취약점 및 사이버 공격의 실제 사례 그리고 기존 제어시스템 침입 탐지 연구에 대하여 서술한다. 3장에서는 본 논문에서 제안하는 산업 제어 시스템을 위한 침입 탐지 시스템을 서술하고 4장에서 침입 탐지 시스템의 성능 검증을 위한 공격 실험과 그 결과를 확인하며 5장에서 결론을 맺는다.

2. 관련 연구

다음 Table 1과 Table 2 그리고 Fig.1은 미국 ICS-CERT에서 산업 제어 시스템의 사고 분야를 조사한 결과와 실제로 산업 제어 시스템을 대상으로 발생한 공격과 실제 피해 사례 그리고 공격 방식이다. Table 1과 Table 2 그리고 Fig.1에서도 확인할 수 있듯이 산업 제어 시스템에 대한 공격은 매년 점점 증가하고 있다. 하지만 발생한 사고의 원인은 대부분이 알 수 없는 새로운 종류의 공격이 계속해서 발생하고 있고 충분한 탐지 및 로깅의 부재로 식별조차 되지 않고 있는 실정이다[3-4]. 이렇게 발견된 사례들 뿐 아니라 발견되지 않은 경우가 더 많을 것으로 예상된다.

Table 1. Statistics of accidents in industrial control system

Sector	2013	2014	2015
Emergency	0	0	10
Energy	19	43	33
Governmnet Facilities	2	5	12
Transportation	10	10	9
Water and Wastewater	23	38	39
Nuclear reactors etc.	8	5	0
Information technology	2	0	3
Total	64	101	106

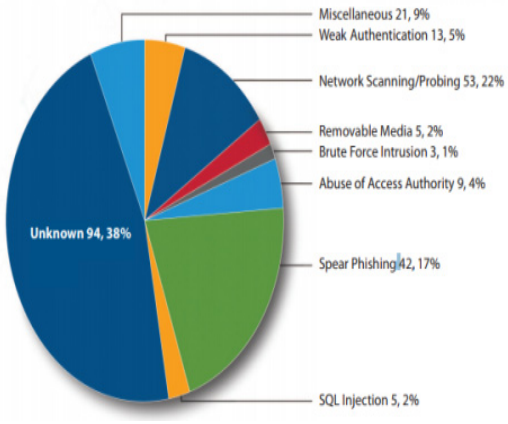

Fig. 1. Attack type statistics for industrial control systems

Table 2. Cases of attack damage to industrial control system

Case	Result
Hacking the Queen-sland sewage treatment plant (2000)	The sewage treatment system was taken over by control, and as a result, a large amount of wastewater was discharged.
Hacking the Davis-Besse nuclear power station (2003)	The SQL server was infected with malware, and the processing computer did not work.
Hacking the Poland Tram control system (2008)	The control system was hacked, resulting in train derailment and injuries of passengers.
Stuxnet (2010)	Destruction of nuclear facilities in Iran caused by malicious code infections.
Havex malware(2014)	Habex malware was found in a Nordic SCADA software provider.
Hacking the Ukraine power plant (2015)	Large scale power outage occurred due to takeover control of power plant.

Table 2에서 확인 가능한 것처럼 대부분의 공격 방식은 데이터를 조작하는 중간자 공격방식의 공격과 정상적인 기능 수행을 방해하는 디도스 공격 그리고 산업 제어 시스템에 특화된 공격인 스턱스넷이 산업 제어 시스템을 대상으로 하는 공격 중 대표적인 공격 방식이다. 산업 제어 시스템의 보안을 위해 방화벽이나 각종 보안 솔루션을 적용하지만 공격방식이 점점 진화함에 따라 계속해서 피해가 발생하고 있다. 따라서 이러한 새로운 공격들을 방어하기 위해 비정상행위들을 탐지하는 침입 탐지 시스템을 적용하고 있다.

하지만 기존의 산업 제어 시스템에 보안 솔루션을 적용하는 것은 기존 시스템의 운영에 문제를 줄 수 있기 때문에 제한되는 경우가 대부분이다. 따라서 기존의 시스템에 영향을 주지 않고 공격을 감지할 수 있는 구성요소가 필요하다. 또한 산업 제어 시스템은 공격 사례에 비추어 볼 때 기존의 알려진 공격이 아닌 전혀 새로운 방식의 공격들이 많이 발생하고 있고 앞으로 점점 진화할 것이다. 따라서 알려진 공격뿐만 아니라 새로운 공격 또한 탐지가 가능한 침입 탐지 시스템의 적용이 필수적이다.

다음은 산업 제어 시스템의 비정상 행위를 탐지하기 위하여 연구한 침입 탐지 시스템이다.

[5]는 산업 제어 시스템에서 발생할 수 있는 이상 징후를 유형별로 분류하고 화이트리스트를 기반으로 이상 징후를 탐지하는 연구로 낮은 오탐율을 가지지만 탐지 범위가 한정된다는 단점이 있다. 네트워크 기반의 탐지 시스템으로 제어시스템의 물리 계층의 탐지는 불가능한 단점을 가지고 있다.

[6]은 많은 기관에서 사용하는 SCADA(Supervisory Control And Data Acquisition) 룰을 수집하여 데이터베이스로 제공하여 이 룰을 사용하여 공격을 탐지하는 방식으로 여러 시스템에 적용이 가능한 장점이 있지만. SCADA 룰을 사용하여 탐지를 하기 때문에 기존의 탐지방식인 알려지지 않은 공격에는 다소 취약한 단점을 가지고 있다.

[7]은 정상적인 시스템 동작을 관찰하여 안전한 영역을 설정하고 그 영역을 벗어나는 경우 탐지하는 방식으로 안전한 영역을 설정하는 기준이 네트워크 패킷의 헤더와 시스템의 CPU 상태를 컴퓨터가 자율적으로 판단하기 때문에 실제 액추에이터가 동작하는 물리 계층에서의 데이터 변화를 감지하는 것이 쉽지 않은 단점이 있다.

[9]는 DDoS 공격을 막기 위한 연구로 적용 시스템마다 환경에 대한 분석이 필요한 단점을 가지고 있다.

본 논문에서는 이러한 문제점을 해결하기 위해 비정상행위를 탐지하는 침입 탐지 시스템을 제안하고 실제 패킷을 스니핑하는 시스템을 구현하여 이전 논문에서 구현한 테스트베드[2]에 적용함으로써 제안한 시스템의 효율성을 검증한다.

3. 제안하는 침입 탐지 시스템

산업 제어 시스템에 적용이 가능하기 위해서는 기존의 시스템에 영향을 주지 않고 공격을 감지할 수 있는 구성요소가 필요하며, 알려진 공격뿐만 아니라 새로운 공격 또한 탐지가 가능한 침입 탐지 시스템이 필수적이다.

따라서 본 논문에서는 기존의 시스템에 영향을 주지 않고 비정상행위를 탐지하는 Fig.2와 같은 행위기반 침입 탐지 시스템을 제안한다. 제안하는 침입 탐지 시스템은 오픈소스 패킷 캡쳐 라이브러리인 WinPcap을 기반으로 구성된다. Pa-cket_sniffer는 각각 물리 프로세스와 PLC(Programmable Logic Controller)간의 통신 패킷과 서버와 PLC간의 통신 패킷을 캡쳐하는 즉, 검사 포인트의 패킷을 스니핑하는 기능을 수행한다.

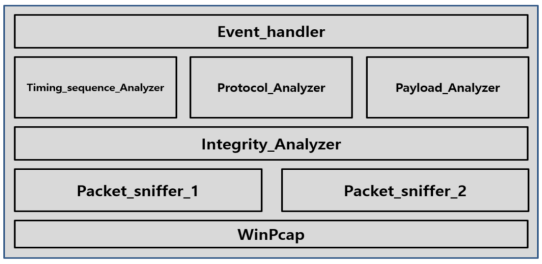

Fig. 2. Architecture of intrusion detection system

Fig.3과 같이 각 구간별로 캡처한 패킷은 integrity_analyzer에서 비교하여 같은 시간에 발생하여 전송된 패킷인지 비교한다. 침입 탐지 시스템은 시스템의 두 구역에서 패킷을 스니핑한다. 각각의 packet_sniffer는 물리 프로세스와 PLC사이의 통신 패킷과 PLC와 서버 사이의 패킷을 스니핑하여 analyzer부로 전달한다.

비교 결과 이상이 없다면 통신의 송수신주기를 분석하는 timing_sequence_analyzer, 통신 프로토콜을 분석하는 protocol_analyzer 그리고 통신 데이터를 분석하는 payload_analyzer에서 탐지 규칙을 적용하여 분석한다.

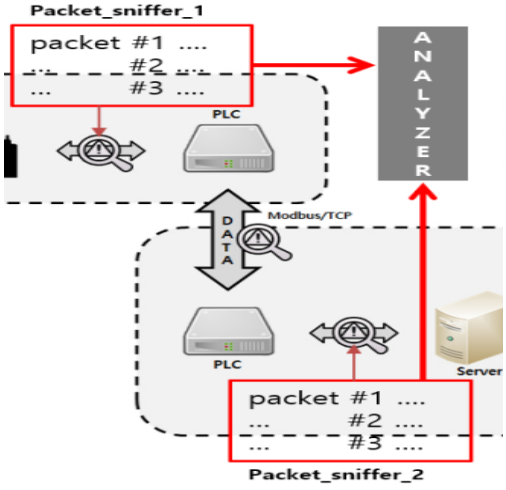

Fig. 3. Process of checking data integrity

제안한 침입 탐지 시스템은 다음 Table 3과 같은 환경과 도구 및 언어를 사용하여 구현하였다. 이전연구[2]에서 구현한 테스트베드는 물리 프로세스 구현을 위해 matlab과 visual studio를 사용하였고 침입 탐지 시스템은 visual studio를 사용하여 구현하였다. 이때 패킷을 스니핑하기 위하여 WinPcap 라이브러리를 사용하였다.

Table 3. Implementation environment and tools of this paper

Implementation	Testbed	Intrusion detection system
Environment	Windows 10	Windows 10
Tools	VS 2015, Matlab(Simulink)	VS 2015
Language	C, C++, Portran	C, C++

본 논문의 침입 탐지 시스템이 비정상 행위를 탐지하기 위한 탐지 조건은 송수신주기, 통신 프로토콜, 패킷의 페이로드로 다음 Table 4와 같이 3가지로 정의하고 각각의 조건에 대하여 탐지 규칙을 정의하였다. 또한 각각의 탐지 조건과 관련 있는 공격을 정리하였다.

Table 4. Detection conditions of intrusion detection system and related attack

	Condition 1	Condition 2	Condition 3
Detection rule	Timing sequence	Communication Protocol	Packet Payload
Related attack	Scanning, Probing, MITM, DDoS	Manipulating, MITM	Stuxnet like attack

산업 제어 시스템은 주기성을 가지며 일정한 데이터를 가지고 통신을 하는 특징을 갖는다. 일반적인 IT 시스템에 비해 송수신주기의 폭은 여유롭지만 정해진 송수신 주기는 엄격하게 지켜야한다. 제어권 탈취 및 디도스 공격의 영향으로 인한 송수신주기의 변화를 탐지하기 위하여 탐지 조건 1로 정의하였다. 본 논문의 침입 탐지 시스템은 송수신주기를 1초로 정의한다.

Modbus 프로토콜은 산업 제어 시스템에서 많이 사용되고 있는 산업 표준 프로토콜 중 하나이다. 감청, 조작 등과 같은 중간자 공격과 같은 탈취 및 침입에 의한 공격에 의해 프로토콜 구조의 손상이 발생할 수 있다. 따라서 캡처한 패킷의 구조를 분석하여 Modbus 프로토콜인지 확인하기 위하여 조건 2로 정의하였다. 다음 Table 5는 Modbus/TCP의 필드들을 나타낸다. 총 6개의 필드를 검사하여 Modbus 표준 프로토콜과 일치하는지 확인하고 transaction 필드를 통해 요청한 패킷에 맞는 패킷을 확인하여 각각의 packet_sniffer가 스니핑한 패킷을 integrity_analyzer에서 비교할 수 있도록 한다.

Table 5. Detection rules of condition 2 (Protocol)

Modbus TCP(read)		Modbus TCP(write)	
field name	function	field name	function
transaction identifier	data processing sequence number	transaction identifier	data processing sequence number
protocol identifier	Modbus TCP -> 0	protocol identifier	Modbus TCP -> 0
length field	length to end of packet	length field	length to end of packet
unit identifier	slave address (255 when not used)	unit Identifier	slave address (255 when not used)
function code	code : 0x03 Modbus read	function code	code : 0x10 Modbus write
data bytes	data information to request	data bytes	transmission data

Payload는 패킷에서 실제 데이터가 저장되어 있는 필드로 어떠한 데이터를 통신하는지 확인할 수 있다. 따라서 검사 포인트의 데이터에 저장되어 있는 payload를 검사하여 스턱스넷 방식의 공격이 탐지 가능하다. 본 논문의 침입 탐지 시스템은 테네시 이스트만 공정을 모델링한 테스트베드에서 검증을 수행하기 때문에 테네시 이스트만 공정의 정상 데이터 범위 내에서 동작하는지 분석하기 위하여 조건 3으로 정의하였다. Table 6는 payload의 데이터를 분석하기 위한 탐지 규칙 중 일부이고, Table 6을 포함하여 총 53개의 항목으로 구성되어 있다.

각각의 데이터는 최소값에서 최대값까지의 값으로 변화할 수 있으며 별도의 시뮬레이션 설정값이 없다면 디폴트 값으로 프리셋되어 전달된다[8]. 침입 탐지 시스템의 payload_analyzer는 패킷의 data bytes 필드 데이터를 검사하여 물리 프로세스의 데이터가 최소값과 최대값 사이에서 동작하는지를 분석한다.

각각의 분석 도구에서 패킷의 분석을 마치고 나면 분석 결과를 event_handler에 전달하고, Table 7과 같이 분석 결과에 따른 이벤트를 발생시켜 사용자에게 알린다. 분석 중 오류인 분석 결과가 발생하면 분석 도구는 더 이상 분석을 진행하지 않고 event_handler에서 오류 메시지를 통해 사용자에게 문제가 있음을 알린 후 다음 패킷을 검사한다.

산업 제어 시스템에서 발생하는 공격 중 시스템 외부 또는 심지어 시스템 내부에서 발생하는 공격은 어느 구간에서 공격이 발생했는지 파악하기가 쉽지 않다. 이처럼 실제 공격의 발생 유무를 파악하지 못하는 경우가 대부분을 차지한다. 때문에 event_handler를 통해 본 논문의 침입 탐지 시스템의 탐지 규칙에 부합하지 않는 패킷으로 통신한 경우 패킷의 어느 필드에 어떠한 문제가 있는지를 사용자에게 알릴 수 있도록 구현하여 사용자가 그에 알맞은 조치를 취할 수 있을 것으로 사료된다.

Table 6. Detection rules of condition 3 (Payload)

Variable	Min.	Max.	Default(%)	Unit
D feed (XMS01)	0	5811	63.053	kg/h^{-1}
E feed (XMS02)	0	8354	53.980	kg/h^{-1}
A feed (XMS03)	0	1.017	24.644	kscm/h
A/C feed (XMS04)	0	15.25	61.302	kscm/h
Compressor valve	0	100	22.210	%
Purge valve	0	100	40.064	%
Separator flow	0	65.71	38.100	m^3/h^{-1}
Stripper flow	0	49.10	46.534	m^3/h^{-1}
Stripper vavle	0	100	47.446	%
Reactor water flow	0	227.1	41.106	m^3/h^{-1}
Condenser water flow	0	272.6	18.114	m^3/h^{-1}
Agitator speed (XMS11)	150	250	50.000	rpm
...	...	...	...	...
Component H (XMS53)	none	none	43.828	mol%

Table 7. Operation of event_handler according to analysis result of each analyzer

Tool	Integrity_analyzer	Timing_.._analyzer
Analysis result	0x00 : normal 0x01 : error	0x00 : normal 0x01 : different from setup time
Generation event	Output error message	Output time and error message
Tool	Protocol_analyzer	Payload_analyzer
Analysis result	0x00 : normal 0x01 ~ 0x06 : no. 1-6 field error	0x00 : normal 0x01 ~ 0x53 : XMS01 ~ XMS53 value error
Generation event	Output the field and error message	Output error value and error message

4. 침입 탐지 시스템 공격 탐지 실험

본 논문에서 제안한 침입 탐지 시스템의 효율성을 검증하기 위해 산업 제어 시스템에서 많이 발생하는 공격 방식을 실험하였다. 산업 제어 시스템에서 주로 발생하고 공격결과가 치명적인 공격인 중간자 공격과 디도스 공격 그리고 스턱스 넷과 유사한 공격 실험을 진행하였다.

본 논문의 침입 탐지 시스템은 유효성을 검증하기 위해 Fig.4와 같이 실제 환경의 산업 제어 시스템의 테스트베드를 사용하였다. 테스트 베드는 물리 프로세스, PLC, 서버, HMI, 히스토리안, 공격자로 구성되며 테스트베드에 대한 정보는 본 논문의 이전연구[2]에서 확인할 수 있다.

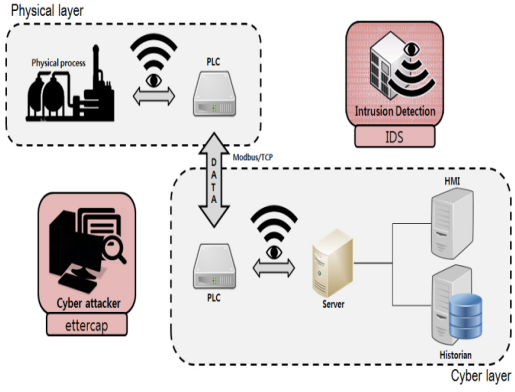

Fig. 4. Testbed configuration with intrusion detection system

공격 실험에 앞서 침입 탐지 시스템의 신뢰성을 검증하기 위하여 컴퓨터 네트워크 분야에서 널리 사용되고 있는 패킷 스니퍼 중 하나인 와이어샤크와 본 논문의 침입 탐지 시스템이 스니핑한 패킷을 비교하여 신뢰성을 확인한다.

Fig.5는 와이어샤크가 스니핑한 패킷이고 Fig.6는 본 논문의 침입 탐지 시스템이 스니핑한 패킷이다. 와이어샤크와 본 논문의 침입 탐지 시스템이 스니핑한 패킷이 동일한 패킷을 스니핑한 것을 Fig.5와 Fig.6에서 확인가능하다. 따라서 본 논문의 침입 탐지 시스템이 수행하는 패킷 스니핑의 신뢰성을 확인하였다.

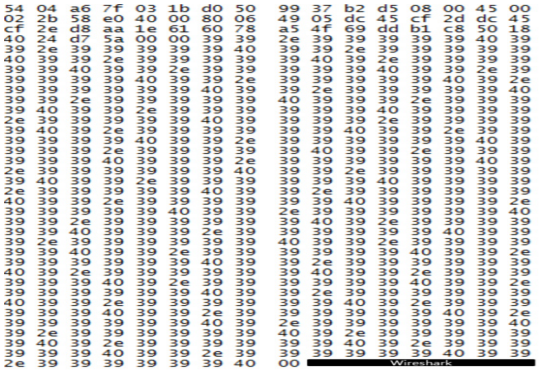

Fig. 5. Packet sniffed by wireshark

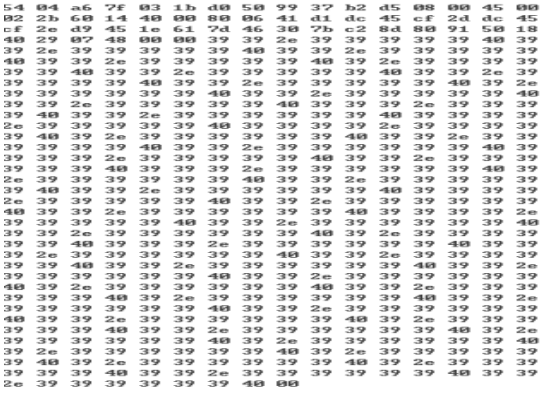

Fig. 6. Packet sniffed by intrusion detection system

공격 실험 시나리오는 다음 Table 8과 같다. 중간자 공격의 경우 공격자가 시스템에 접근하여 스니핑하는 패킷을 무작위로 변형하여 재전송하는 공격을 실험하였다. 디도스 공격 실험의 경우 외부 공격자가 시스템의 마비

Table 8. Scenario of attack experiment

Attack type	Scenario
Man-in-the-Middle (MITM) attack	An attacker who has no knowledge of the protocol structure or system intercepts data from outside, randomly transforms it, and then retransmits it.
DDoS attack	A random TCP SYN flooding attack on the PLC by an external attacker to paralyze the system
Stuxnet-like attack	An attack that sends malicious data to a physical process due to malicious code infection inside the system and sends normal data to the server

를 목적으로 PLC에 무작위 TCP SYN 플러딩 공격을 했을 경우이다[9]. 스턱스넷 유사 공격 실험의 경우 사이버계층의 PLC가 감염되었다는 것을 전제로 물리 계층으로는 조작된 악의적인 데이터를 전송하고 서버로는 정상적인 데이터로 조작된 데이터를 전송하는 공격을 실험하였다. 공격 실험 대상은 이전연구[2]와 마찬가지로 물리 프로세스의 반응기 압력 값의 변화를 관찰하였다.

다음 Fig.7은 정상 상태로 동작한 테스트베드에 침입 탐지 시스템을 적용하지 않은 상태의 반응기 압력 값으로 정상 상태의 동작은 2,700 ~ 2,800kPa의 값을 유지한다.

각각의 공격 실험 시 침입 탐지 시스템을 적용하지 않은 상태에서 테스트베드 구성요소인 히스토리안에 저장된 데이터를 확인하였다.

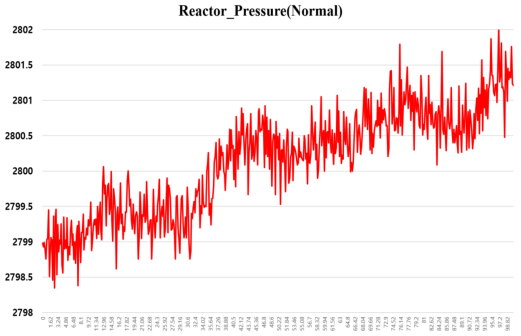

Fig. 7. Normal-state reactor pressure data stored in the historian

다음 Fig.8은 본 논문에서 실험한 중간자 공격의 도식도이다. 물리계층과 사이버계층 사이에서 통신하는 패킷을 가로채어 패킷의 페이로드에 저장되어 있는 반응기 압력 값을 조작하는 공격을 실험하였다.

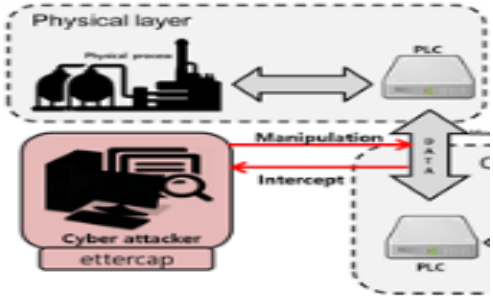

Fig. 8. Experiment process of man in the middle attack

공격 결과 침입 탐지 시스템을 이용하여 비정상행위를 탐지 하지 않았을 경우 히스토리안에 저장된 데이터는 다음 Fig.9와 같다. 침입 탐지 시스템을 적용한 결과 침입 탐지 시스템은 다음 Fig.10과 같이 탐지하였다.

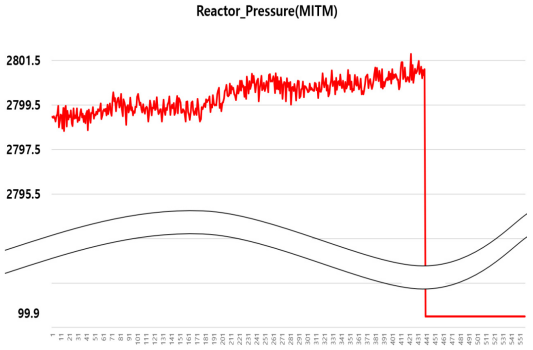

Fig. 9. MITM-state reactor pressure data stored in the historian

위 경우는 페이로드 내부의 모든 데이터를 아스키 코드로 변환하여 모든 정수 값을 0x63으로 치환하여 재전송한 공격이다. 따라서 통신 주기와 페이로드 크기는 규칙에 위배되지 않은 것을 확인할 수 있고 페이로드에 저장된 물리 프로세스 데이터 값만 변한 것을 Fig.10에서 확인할 수 있다.

다음 Fig.11는 디도스 공격을 실험의 도식도이다. 사이버계층의 PLC를 향해 SYN 플러딩 공격을 실험하였고 침입 탐지 시스템을 적용하지 않았을 경우 히스토리안에 저장된 데이터는 다음 Fig.12와 같다.

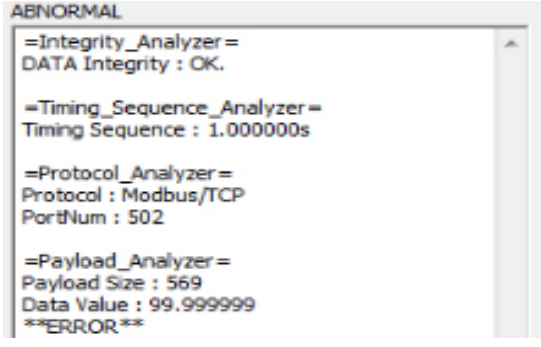

Fig. 10. Detection of intrusion detection system in case of an man in the middle attack

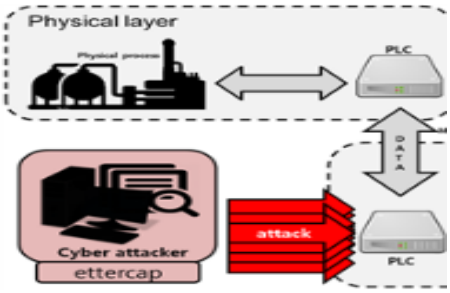

Fig. 11. Experiment process of DDoS attack

PLC를 향한 디도스 공격 방식인 SYN 플러딩 공격의 영향으로 인해 통신주기가 지연되어 계속해서 같은 값이 저장된 것을 확인 할 수 있다.

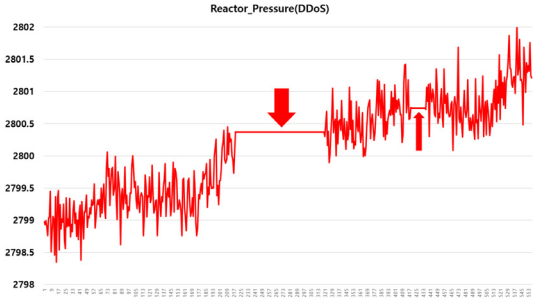

Fig. 12. DDoS-state reactor pressure data stored in the historian

침입 탐지 시스템을 적용하였을 경우에는 통신주기의 지연 발생 유무를 탐지하여 사용자가 공격에 대처할 수 있도록 Fig.13과 같이 이벤트를 발생시키는 것을 확인할 수 있다.

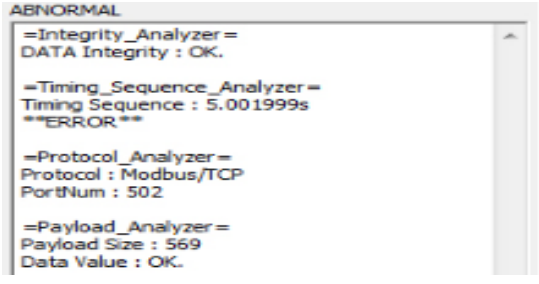

Fig. 13. Detection of intrusion detection system in case of DDoS attack

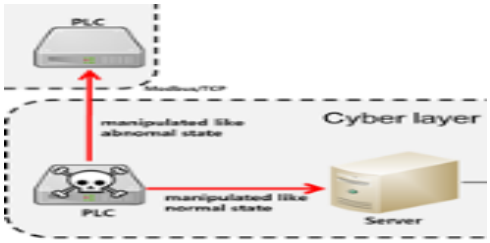

Fig. 14. Experiment process of attack like stuxnet

다음 Fig.14는 스턱스 넷과 유사한 공격 실험을 나타낸다. 시스템 내부 악성코드 감염으로 인해 PLC가 악성코드에 감염되었고, 그 결과 물리 계층에 악의적으로 조작된 데이터를 전송하고 서버에 정상적으로 조작된 데이터를 전송하여 시스템 관리자가 물리 계층의 상태를 알 수 없도록 하는 공격이다.

공격 시 히스토리안에 저장된 데이터는 다음 Fig.15와 같다.

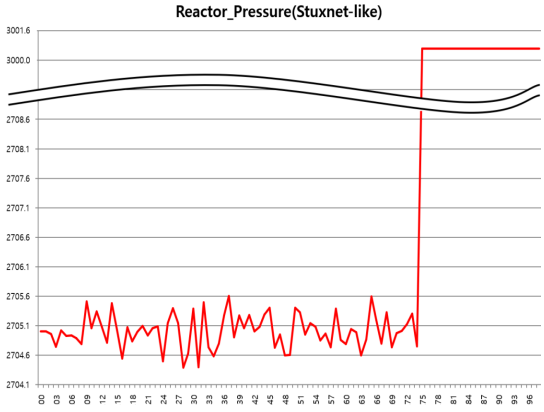

Fig. 15. Stuxnet like attack-state reactor pressure data stored in the historian

반응기 압력 값이 정상적인 값을 유지하던 중 악성코드에 감염된 PLC는 물리 프로세스로 비정상 상태의 반응기 압력값을 전송한다. 그 후 반응기 압력 값이 3,000kPa가 넘는 값을 유지하는 것을 확인 할 수 있다. 이 때 히스토리안에는 조작된 데이터가 저장되기 때문에 packet_sniffer가 수집한 데이터를 가공하여 확인하였다.

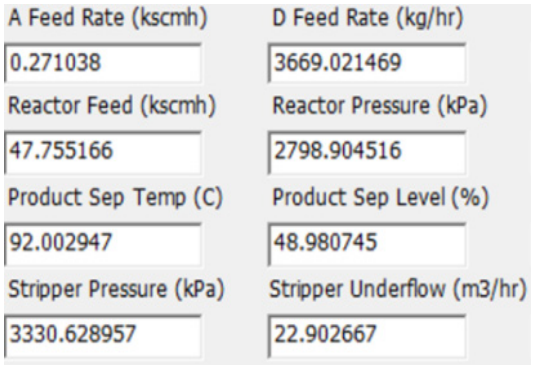

Fig. 16. Experiment process of attack like stuxnet

히스토리안에 저장된 반응기 압력 값은 Fig.16과 같이 실제로는 비정상 값이지만 정상적인 것처럼 조작된 데이터가 저장되기 때문에 시스템 사용자는 실제 공격의 발생유무를 원격에서 확인할 수 없다. 따라서 침입 탐지 시스템을 적용하였고 그 결과 침입 탐지 시스템은 Fig.17과 같이 탐지하였다.

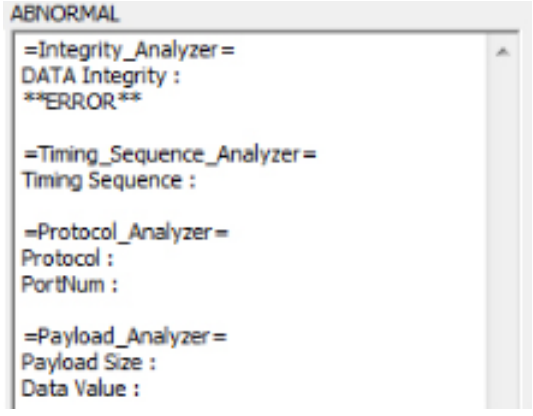

Fig. 17. Detection of intrusion detection system in case of attack like stuxnet

Fig.17은 악성코드에 감염된 PLC는 물리 계층과 사이버 계층으로 서로 다른 데이터를 전송하기 때문에 integrity_analyzer에서 검사 포인트의 패킷을 비교하여 불일치를 탐지한 결과이다.

다음 Table 9는 기존의 침입 탐지 시스템과 본 논문의 침입 탐지 시스템을 비교한 것으로 트래픽 검사, 실제 환경 적용 여부, 유연성과 신뢰도 그리고 본 논문에서 실험한 공격 실험의 탐지 유무에 대하여 비교하였다.

Table 9. Comparison of intrusion detection system

	Ours	[5]	[6]	[7]
Check Point Between Physical System & PLC	O	X	X	X
Real environment	O	X	O	O
Flexibility	H	H	H	L
Scalability	H	H	L	L

기존의 침입 탐지 시스템은 실제 액츄에이터 및 센서가 동작하는 물리 계층과 PLC간의 페이로드를 검사하지 않는다. 이에 따라 액츄에이터가 동작하는 물리 프로세스 영역과 시스템을 관리하는 사이버 영역의 서버에서 실제로는 서로 다른 데이터이지만 같은 데이터로 속이는 스턱스넷 류의 공격을 탐지하기 쉽지 않기 때문에 이 구간을 검사 포인트로 설정하고 이 구간에서의 데이터 검사 유무를 비교하였다. 그리고 산업 제어 시스템에 적용하는 만큼 실제 또는 유사환경에서의 실험이 이루어지는 것이 시스템의 신뢰도 측면에서 매우 중요하기 때문에 실제 환경의 시스템에 적용 유무를 비교하였다. 또한 유연성 및 확장성은 다른 시스템의 적용가능성 및 탐지 규칙의 수정의 용이성을 기준으로 비교한 것으로, 본 논문에서 제안한 침입 탐지 시스템은 각각의 analyzer로 구성되어 있어 다른 시스템에 적용하는 것이 어렵지 않고, 이에 따른 탐지 규칙 수정 또한 각 analyzer별로 수정이 가능하기 때문에 다른 침입 탐지 시스템에 비해 유연하다고 할 수 있다.

위와 같은 실험 결과를 토대로 2장에서 서술한 [5-7]의 침입 탐지 시스템과 본 논문의 침입 탐지 시스템과 비교하였다.

[5]의 침입 탐지 시스템은 화이트리스팅 기법을 사용하여 화이트리스트의 수정만으로 간단하게 탐지 규칙의 수정이 가능하고 화이트리스트에 위배되는 행동들은 엄격하게 탐지가 가능하기 때문에 높은 신뢰도를 가지지만, 물리 계층과 PLC 사이의 포인트를 감시하지 않기 때문에 스턱스 넷 류의 공격 탐지가 어려운 단점을 가지고 있다. 또한 실제 환경에서의 적용에 대한 연구가 미흡한 단점이 있다.

[6]은 실제 환경에서 발생하는 공격에 대한 사용자들의 정보 공유로 생성한 규칙을 토대로 탐지하기 때문에 유연성은 좋지만, 새로운 환경에서는 정보 공유의 단계

를 수행해야하기 때문에 확장성이 떨어진다고 볼 수 있다. 또한 물리 계층과 PLC 사이의 포인트를 감시하지 않기 때문에 스텍스 넷 류의 공격 탐지가 쉽지 않다.

[7]은 자율 컴퓨팅 기술을 사용하여 컴퓨터 스스로 판단하기 때문에 새로운 공격에 대한 탐지 규칙의 수정이 용이하지 않고 다른 시스템에 적용한다고 하여도 자율컴퓨터가 학습할 수 있는 환경과 시간이 필요하기 때문에 확장성도 떨어진다고 볼 수 있다. 또한 물리 계층과 PLC 사이의 포인트를 감시하지 않기 때문에 스텍스 넷 류의 공격 탐지가 쉽지 않은 단점이 있다.

5. 결 론

본 논문에서는 기존의 제어 시스템에 영향을 주지 않고 비정상행위를 탐지하는 제어시스템용 행위기반 침입 탐지 시스템을 제안하고 제안한 시스템을 구현하여 테스트베드에 적용함으로써 제안한 시스템의 효율성을 검증하였다. 본 논문에서 제안하는 침입 탐지 시스템은 크게 세 가지의 규칙을 통해 규칙에 위배되는 패킷을 탐지하였다. 테스트베드의 통신주기, 페이로드 크기, 페이로드 내부의 데이터 값을 정상적인 상황에서의 시뮬레이션 데이터를 토대로 탐지 규칙을 생성하고 생성된 규칙에 의해 발생할 수 있는 비정상행위를 탐지하였다. 침입 탐지 시스템의 신뢰성을 확인하기 위해 와이어샤크로 스니핑한 패킷과 비교하여 확인하였고 공격 실험 결과 공격의 탐지가 가능한 것을 확인하였다.

하지만 점점 더 진화하는 공격 방식에 따라 여러 공격을 시스템에 적용하여 침입 탐지 시스템을 발전시킨다면 효율적인 침입 탐지 시스템이 될 것이라고 사료된다.

References

[1] Fireeye Inc., "2017 Security Predictions", Technical Report, Dec. 2016.

[2] Hyun-Seok Kim and Dong-Gue Park, "Implementation of the testbed for security of industrial control system", *Journal of KIIT*, vol. 15, no. 6, pp. 53-60, Jun. 2017. DOI: https://doi.org/10.14801/jkiit.2017.15.6.53

[3] NCCIC, "ICS-CERT Monitor", Technical report, Feb. 2015.

[4] Do-Yeon Kim, "Vulnerability analysis for industrial control system cyber security", *Journal of JKIECS*, vol. 9, no. 1, pp. 137-142, Sep. 2014. DOI: https://doi.org/10.13067/JKIECS.2014.9.1.137

[5] Hyunguk Yoo, Jeong-Han Yun, and Taeshik Shon, "Whitelist-based anomaly detection for industrial control system security", *Journal of KICS*, vol. 38, no. 8, pp. 641-653, Oct. 2013. DOI: https://doi.org/10.7840/kics.2013.38B.8.641

[6] Jan Vavra and Martin Hromada, "Comparison of the Intrusion Detection System Rules in Relation with the SCADA Systems", *Proc. of 5th Computer Science On-line Conference (CSOC 2016)*, vol. 465, pp. 159-169, Apr. 2016. DOI: https://doi.org/10.1007/978-3-319-33622-0_15

[7] Qian Chen, Sherif Abdelwahed, and Abdelkarim Erradi, "A model-based approach to self-protection in computing system", *Proc. of the 2013 ACM Cloud and Autonomic Computing Conference*, no. 16, pp. 1-10, New York, USA, 2013. DOI: https://doi.org/10.1145/2494621.2494639

[8] J. J. Downs and E. F. Vogel, "A plant-wide industrial process control problem", *Journal of Computers & chemical engineering*, vol. 17, no. 3, pp. 245-255, 1993.

[9] Hyung-Su Lee, and Jae-Pyo Park, "Respond System for Low-Level DDoS Attack", *Journal of the Korea Academia-Industrial cooperation Society*, vol. 17, no. 10, pp. 732-742, 2016. DOI: http://dx.doi.org/10.5762/KAIS.2016.17.10.732

김 현 석(Hyun-Seok Kim) **[학생회원]**

- 2016년 2월 : 순천향대학교 정보통신공학과(공학사)
- 2018년 2월 : 순천향대학교 정보통신공학과 석사

<관심분야>
제어 시스템 보안, 정보 보안, 컴퓨터 네트워크

박 동 규(Dong-Gue Park) **[정회원]**

- 1985년 2월 : 한양대학교 전자공학과(공학사)
- 1988년 2월 : 한양대학교 전자공학과(공학석사)
- 1992년 2월 : 한양대학교 전자공학과(공학박사)
- 1992년 3월 ~ 현재 : 순천향대학교 정보통신공학과 교수

<관심분야>
제어 시스템 보안, 애플리케이션 보안, 보안 관제