한국통신학회논문지 '13-08 Vol.38B No.08
http://dx.doi.org/10.7840/kics.2013.38B.8.641

제어시스템 보안을 위한 whitelist 기반 이상징후 탐지 기법

유 형 욱◆, 윤 정 한*, 손 태 식°

Whitelist-Based Anomaly Detection for Industrial Control System Security

Hyunguk Yoo◆, Jeong-Han Yun*, Taeshik Shon°

요 약

최근 제어시스템을 대상으로 한 사이버공격이 점차 고도화·지능화됨에 따라 기존 시그니처(signature) 기반 탐지 기법은 한계에 봉착하였고, 이에 제어시스템 환경에 적합한 화이트리스트(whitelist) 기반 보안 기법이 새롭게 주목받고 있다. 그러나 최근 개발되고 있는 화이트리스트 기법들은 어플리케이션 레벨에서 한정적으로 사용되고 있으며, 무엇보다 블랙리스트(blacklist) 기반 보안 기법과 달리 이상 징후 유형에 대한 구체적 정보 제공이 불가능하다는 단점이 존재한다. 본 논문에서는 제어시스템에서 발생할 수 있는 이상 징후 유형들을 분류하고, 네트워크 레벨에서의 화이트리스트를 통해 이상 징후를 탐지할 수 있는 모델을 제시한다.

Key Words : Industrial Control System, SCADA, Whitelist, Anomaly Detection, Cyber Attack Taxonomy

ABSTRACT

Recent cyber attacks targeting control systems are getting sophisticated and intelligent notoriously. As the existing signature based detection techniques faced with their limitations, a whitelist model with security techniques is getting attention again. However, techniques that are being developed in a whitelist model used at the application level narrowly and cannot provide specific information about anomalism of various cases. In this paper, we classify abnormal cases that can occur in control systems of enterprises and propose a new whitelist model for detecting abnormal cases.

Ⅰ. 서 론

제어시스템은 생산의 자동화가 이루어진 공장을 비롯한 교통 관리, 전력 생산, 자원 관리 등 국가 기반 시설 전반에 걸쳐 널리 사용되고 있다. 게다가 제어시스템을 통해 제어되는 요소들은 국방, 항공 등 보다 넓은 분야에 걸쳐 활용되고 있으며, 특히 차세대 IT 전력망인 스마트그리드의 제어시스템은 기존의 전력망과 더불어 IT 기술을 접목하여 구성요소 간 제어관리 체계의 유기성을 극대화하였다. 이와 같이 제어시스템의 기술 고도화 및 시스템 간 커뮤니케이션 채널 생성을 통한 데이터 공유가 이루어지면서 제어시스템 보안에 대한 중요도와 그 가치는 시간이 지날수록 보다 높아지고 있다.

과거의 제어시스템은 외부 네트워크와 분리되어 한정된 소수의 사람만이 접근할 수 있는 환경에 설치 및 운영되었다. 하지만 최근의 제어시스템은 정보통신 기술을 접목하여 네트워크를 통한 원격제어 및 자동제어

◆ 주저자 : 아주대학교 컴퓨터공학과, cielo1025@ajou.ac.kr, 학생회원
° 교신저자 : 아주대학교 정보컴퓨터공학과, tsshon@ajou.ac.kr, 정회원
* 한국전자통신연구원 부설연구소, dolgam@ensec.re.kr
논문번호 : KICS2013-04-187, 접수일자 : 2013년 4월 25일, 최종논문접수일자 : 2013년 6월 28일

가 일반화 되고 있다. 특히 스마트그리드의 제어시스템은 IT 네트워크를 통한 데이터 통신을 중추적인 기술로 적용하여 자동화 변전소 등의 제어에 사용한다. 이와 같은 제어시스템의 발전은 효율성 측면에서 많은 이점을 가지고 있지만, 보안적인 측면에서 보았을 때 과거에 비해 많은 취약점을 내포하게 되었다. Modbus, DNP3와 같이 인증 또는 암호화 메커니즘이 고려되지 않고 설계된 제어시스템 통신 프로토콜을 사용하거나 보안 코딩(secure coding) 등이 적용되지 않은 여러 제어시스템 제품들은 현재 심각한 보안 위협에 직면해 있다. 2013년 NSS 연구소에서 발표한 「Vulnerability Threat Trends」에 따르면 공개된 SCADA 관련 취약점이 2010년 20개에서 2013년 124개로 600%가량 급증한 것을 알 수 있다. 이는 현재까지 공개된 수치일 뿐이며 아직 발견되지 않은 취약점까지 포함한다면 이보다 훨씬 많을 것으로 추정된다.

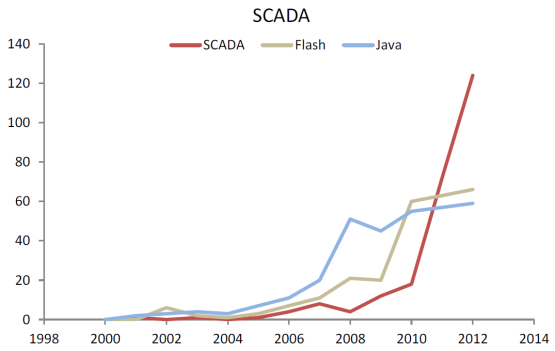

그림 1. SCADA 취약점 증가 추세 1)
Fig. 1. Changes in Vulnerabilities of SCADA

한편, 제어시스템 취약점을 이용한 최근의 사이버 공격들은 갈수록 고도화·지능화 되고 있는 추세이다. 지난 2010년 등장한 스턱스넷(Stuxnet)은 대표적인 제어시스템 대상의 APT 공격으로 다수의 제로데이(zero-day) 취약점을 이용하였다고 알려져 있다.2) 제로데이 취약점을 이용한 공격, APT(Advanced Persistent Threat), 고도화된 다형성(polymorphism) 기법을 사용한 악성코드 앞에서 기존 시그니처(signature) 기반 방어 솔루션은 한계를 드러내고 있다.

최근에는 이러한 고도화된 사이버공격으로부터 제어시스템을 보호하기 위한 방안 중 하나로 화이트리스트(whitelist) 기반 보안 기법이 고려되고 있다. 화이트리스트 보안 기법은 시스템의 정상 행동을 화이트리스트로 정의하고 이에 반하는 모든 행위를 제한하는 방법으로 보안성은 매우 높지만 오경보(false alarm)율이 높아 일반적인 IT 시스템에서는 사용이 제한되어 왔다. 하지만 제어시스템 환경에서는 시스템 동작 패턴 또는 네트워크 통신 트래픽이 규칙적이기 때문에 화이트리스트 기법의 적용이 효과적일 수 있으며, 국내외 관련 벤더들은 이미 화이트리스트 기반 보안 제품들을 출시하고 있다.

그러나 현재 알려진 화이트리스트 방식의 제품들은 주로 개별 호스트에서의 어플리케이션 제어에 초점이 맞춰져 있기 때문에 네트워크 레벨에서의 세부적인 탐지를 수행하지 못한다. 일부 진화된 제어시스템 방화벽 제품에서는 제어시스템 통신 프로토콜 특성에 따라 세부적인 패킷 검사를 수행하고 있지만 규칙에 존재하지 않는 패킷에 대해 단순히 차단을 할 뿐 그것이 구체적으로 어떤 위협인지 정보를 주지 못하기 때문에 보안 관리자 입장에서 효과적인 대응이 어렵다.

본 논문에서는 제어시스템에서 발생할 수 있는 이상 징후 유형들을 분류하고, 네트워크 레벨에서의 화이트리스트를 통해 이상 징후를 탐지할 수 있는 모델을 제시함으로써 기존 화이트리스트 방식의 단점을 보완하였다. 논문의 구성은 다음과 같다. 2장에서 기존 화이트리스트 관련 연구들을 소개하고, 3장에서 제어시스템 환경에서 발생할 수 있는 사이버공격 및 오동작 유형에 대해 분류한다. 4장에서는 제어시스템 네트워크 레벨에서 적용 가능한 화이트리스트 규칙을 정의하고, 이를 이용한 탐지 모델을 제시한다. 5장에서는 간단한 시나리오를 통해 제안한 모델의 유효성을 입증하고 마지막 6장에서는 본 논문의 결론을 맺고 향후 연구 방향에 대해 논의한다.

Ⅱ. 관련 연구

제어시스템 환경에서의 블랙리스트 기반 보안 기법의 한계에 따라 화이트리스트 기반 기법의 적용이 많이 논의되고 있다[1,2]. 현재 주로 사용되고 있은 제어시스템 화이트리스트 방식은 크게 어플리케이션 화이트리스트 기법과 화이트리스트 규칙을 사용한 방화벽 정도로 구분할 수 있다. 어플리케이션 화이트리스트 기법은 개별 호스트에서 허용된 정상 어플리케이션들을 정의하고, 이에 해당하지 않는 어플리케이션의 실행을 금지하는 방법으로 관련 제품으로는 AhnLab의 TrusLine, McAfee社의 Application Control, Industrial

1) Stefan Frei, "Vulnerability Threat Trends", NSS Lab., 2013
2) 스턱스넷 공격에 사용된 6개의 취약점 중 5개(CVE-2010-2568 CVE-2010-2729, CVE-2010-2743, CVE-2010-2772, CVE-2010-3338)가 제로데이 취약점이었음

Defender社의 HIDS 등이 있다. 최근 몇몇 진화된 제어시스템 방화벽 제품에서는 기존의 단순한 MAC, IP, Port 기반 화이트리스트 규칙과 더불어 특정 제어 통신 프로토콜(Modbus, DNP3, ICCP 등)에 대한 프로토콜 스펙 수준의 세부적 트래픽 감시를 지원하고 있다. 이와 관련된 제품으로는 Tofino社의 Modbus DPI Firewall가 대표적이다.

2.1. Ahnlab, 「TrusLine」

Ahnlab 'TrusLine'은 시스템의 안정적 운용에 대한 민감도가 높아 정해진 프로그램만 사용하는 산업용 제어시스템에 최적화된 화이트리스트 기반 보안 솔루션으로 다음과 같은 특징이 있다.

- 허가되지 않은 어플리케이션 설치 제한 (application control)
- IP/Port 차단 및 외부 저장장치 자동 실행 방지를 통한 감염 경로 차단
- OS 패치 및 업데이트와의 독립성 제공
- 제어시스템 메모리/CPU 점유율 최소화

2.2. McAfee, 「Application Control」

McAfee社의 'Application Control' 및 'Change Control' 역시 어플리케이션 화이트리스트 기반의 제어시스템 보안 솔루션으로 아래와 같은 특징이 있다.

- 광범위한 운영체제 지원(Window, Linux, UNIX, POS 단말기 OS, Window CE)
- 신뢰모델을 이용한 동적 화이트리스트 생성
- 파일 및 폴더 무결성 감시
- 불법적인 스크립트 및 드라이버 실행 차단 (메모리 감시)
- 레지스트리 키 및 중요 구성 파일의 변경 방지

2.3. Industrial Defender, 「HIDS」

Industrial Defender社가 CoreTrace社와 기술협약을 통해 개발한 CoreTrace Bouncer 6-Based HIPS (Host Intrusion Prevention System)은 화이트리스트 기반 제어시스템 전용 침입방지시스템으로 ABB, GE Energy, Itron 등의 글로벌 스마트그리드·전력기기 업체들에 제공되고 있으며 다음과 같은 특징이 있다.

- 화이트리스트 기반 어플리케이션 설치 및 동작 제어
- 네트워크 트래픽 영향 최소화
- 소프트웨어 업데이트 시 동적 화이트리스트 추가
- NERC-CIP compliance 준수

2.4. Tofino, 「Modbus DPI Firewall」

정통적인 방화벽은 송·수신 IP 주소 및 Port 번호 정도를 검사하였다. 하지만 이런 방화벽의 경우 정상 IP 주소 및 Port 번호로 위장한 공격에 대해서는 검사 하지 못한다는 단점이 있었다. Tofino社에서 개발한 방화벽은 제어시스템 프로토콜 따라 정상적인 메시지 포맷을 갖추고 있는지 여부 및 허용된 제어 메시지를 보내는지 등을 검사함으로써 강력한 보안성을 제공한다. 예를 들어 Honeywell Modbus Read-only Firewall와 같은 Modbus DPI Firewall은 Modbus 메시지의 read/write 여부를 검사하여 모든 write 메시지를 필터링한다.

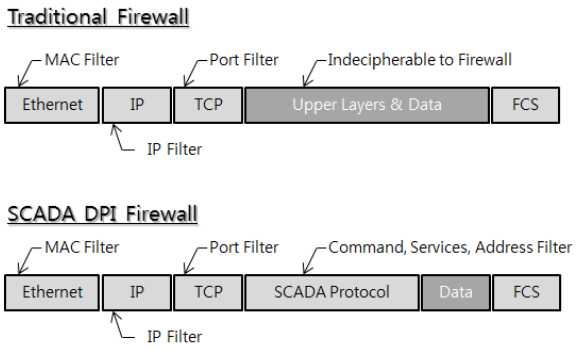

그림 2. Traditional Firewall vs. SCADA DPI Firewall
Fig. 2. Traditional Firewall vs. SCADA DPI Firewall

어플리케이션 화이트리스트 방식은 호스트 시스템에서 동작하기 때문에 호스트 환경에 의존적이며, 이에 따라 소프트웨어 설치 및 업그레이드로 인한 일시적 서비스 중단, 성능 저하 문제 등이 야기될 수 있다. 한편 현재 제어시스템 방화벽에서 사용되고 있는 네트워크 기반 규칙들을 통해 이상 패킷들을 효과적으로 차단할 수는 있지만, 해당 패킷들이 어떤 유형의 공격 또는 오동작인지 파악하기가 어렵다는 단점이 존재한다. 특히 기존 화이트리스트 방식은 정상 행위 규칙을 어긴 모든 이벤트들을 차단할 수는 있지만, 차단된 이벤트들이 어떤 유형의 공격 또는 오동작인지에 대한 세부 분류가 어렵기 때문에 보안 관리자 입장에서의 대응이 어렵다.

Ⅲ. 제어시스템 이상 징후 유형 분류

본 논문에서는 화이트리스트 기반 이상 징후 탐지 모델을 제시하기 위해 먼저 제어시스템 환경에서 발생할 수 있는 공격 및 오동작 유형을 분류하였다. 제어시스템에서 발생 가능한 이상 징후 유형을 가능

한 전수 조사 및 분류하기 위해 관련 연구 논문들과 [3][4][5][6][7], 미국 국토안보부에서 발표한 산업제어시스템 취약점 보고서[8], IEC 62351 Part1[9], Digital Bond社에서 발표한 스카다 IDS 규칙[10] 등을 조사하였다. [3]에서는 제어시스템에 대한 사이버 공격을 크게 하드웨어에 대한 공격, 소프트웨어에 대한 공격, 통신 스택(communication stack)에 대한 공격으로 나누어 분류하였고, 세부 공격 유형으로 버퍼 오버플로우, SQL Injection, Idle Scan, Smurf, ARP Spoofing 등을 소개하였다. [4]에서는 Modbus, DNP3 프로토콜에 관련된 취약점과 이를 이용한 서비스 거부 공격(Denial of Service Attack), 중간자 공격(Man-In-the-Middle Attack), 재전송 공격(Replay Attack) 등에 대해 나열하였다. [5]에서는 제어시스템에서 발생할 수 있는 사이버 위협요인 32가지를 제어센터 내부, 통신 링크, 제어 장치(IED, RTU, PLC 등) 각각의 발생할 수 있는 위치로 분류하였다. [6]에서는 ICCP(Inter-Control Center Communication) 프로토콜을 사용하는 제품에서 발견된 취약점과 이를 이용한 공격 방법들에 대해 소개하였다. [7]은 POSCO社 의 철강 제조 공정 네트워크를 대상으로 실제 공정 망에서 발생하는 통신 장애 유형을 조사하고 이를 탐지하기 위한 모델을 제시하였다. [8]은 제어시스템에서의 취약점을 소프트웨어 취약점, 보안 설정에서의 취약점, 네트워크 취약점으로 크게 구분하고 각각에서의 세부 취약점 유형과 이를 토대로 발생할 수 있는 공격 유형들을 간략히 언급하였다. [9]는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability), 부인 방지(Non-repudiation) 각각의 보안 요구사항과 이와 관련한 보안 위협 그리고 사이버 공격 유형들 간의 관계를 간단히 도식화하였다. [10]에서는 Modbus, DNP3, EtherNet/IP(Ethernet Industrial Protocol) 프로토콜의 취약성을 이용한 공격 시나리오와 시스템 영향도 등을 설명하였고 이를 탐지하기 위한 스노트(Snort) 기반 규칙을 제시하였다. 이 외에도 공격 특징을 분석하기 위해 Metasploit의 SCADA 관련 exploit을 참조하였다.

본 논문에서는 앞서 나열한 여러 제어 시스템 대상 사이버 공격 및 오동작 관련 자료들을 토대로 제어시스템에서 발생 가능한 이상 징후 유형 111개를 도출하고 이를 다시 이용한 취약점에 따라 15개 그룹으로 분류하였다.

표 1. 제어시스템 이상 징후 유형 그룹
Table 1. Groups for Anomaly Symptom of SCADA

Category		Group
Attacks using Vulnerabilities of Firewall Setting		Unauthorized Network Access
		Unauthorized Communication
		Unauthorized Service
Attacks using Vulnerabilities of Software		Buffer Overflow
		Invalid Input Value
Attacks using Vulnerabilities of Protocol Design	SCADA Protocol	Modbus Protocol Attack
		DNP3 Protocol Attack
		GOOSE Protocol Attack
		MMS Protocol Attack
		ICCP Protocol Attack
	TCP/IP	TCP/IP - Spoofing
		TCP/IP - Scanning
		TCP/IP - Others
Flooding		Flooding
Fault		Fault

○ Unauthorized Network Access

공격자가 제어 네트워크의 특정 장치를 공격하기 위해서는 먼저 해당 장치가 존재하는 제어 네트워크로의 연결이 필요하다. 이 때 공격자의 위치는 외부 네트워크(business network, remote control network) 또는 내부 네트워크가 될 수 있으며, 이러한 공격자의 위치와 공격 장비의 주소(IP/MAC)가 허가된 장비 주소인지 여부에 따라 9가지 비정상 연결 케이스가 발생한다. UA2, UA5, UA8의 경우 송신 주소가 내부 또는 외부 네트워크에서 허가된 장비 주소인데 이는 공격자가 허가된 장비에 불법적으로 접근하여 공격 경로로 이용한 경우이거나 주소 스푸핑(IP spoofing, ARP spoofing) 공격 등이 복합적으로 이루어진 경우로 다른 케이스에 비해 심각도(severity)를 높게 부여해야 한다. 마찬가지로 비정상 연결 패킷의 송신 주소가 내부 네트워크일 경우, 공격이 내부 네트워크로부터 이루어지고 있음을 의미하기 때문에 더 신속하게 대응하여야 한다.

표 2. 허가되지 않은 장비를 이용한 공격
Table 2. Attacks of Using Unauthorized Device

ID	Attack Name
UA1	Unauthorized External → Authorized Internal
UA2	Authorized External → Unauthorized Internal
UA3	Unauthorized External → Unauthorized Internal
UA4	Unauthorized Internal → Authorized External
UA5	Authorized Internal → Unauthorized External
UA6	Unauthorized Internal → Unauthorized External
UA7	Unauthorized Internal → Authorized Internal
UA8	Authorized Internal → Unauthorized Internal
UA9	Unauthorized Internal → Unauthorized Internal

○ Unauthorized Communication

공격자가 내부 또는 외부 네트워크에서 허가된 정상 장비 주소를 이용해 비정상 연결을 시도하는 경우는 Unauthorized Communication 공격에 속하게 된다. 즉, 이 경우는 송신 및 수신 장비의 주소 각각은 모두 허가된 장비이지만 두 장비간의 연결이 허가되지 않은 케이스가 된다. 이 때 연결 방향에 따라 [표 3]과 같이 3가지 케이스로 분류될 수 있다.

표 3. 허가되지 않은 통신
Table 3. Attacks of Using Unauthorized Communication

ID	Attack Name
UC1	Unauthorized Communication-A (External → Internal)
UC2	Unauthorized Communication-B (Internal → External)
UC3	Unauthorized Communication-C (Internal → Internal)

○ Unauthorized Service

Unauthorized Service를 이용한 공격은 송·수신 장비 주소가 모두 허가된 장비이고, 두 장비 간 연결 또한 허가되었지만 허가되지 않은 서비스 포트를 이용하는 경우이다. 공격자는 두 장비 간에 허가된 서비스 포트 외에 다른 포트를 이용하여 악성 코드 다운로드, 제어 명령 전달, 정보 수정, 정보 유출 등을 위한 채널로 이용할 수 있다. 허가되지 않은 서비스를 시도하는 두 장비의 종류(외부 서버, 내부 서버, 현장제어장치)에 따라 [표 4]와 같은 8가지 케이스로 구분할 수 있다.

표 4. 허가되지 않은 서비스
Table 4. Attacks of Using Unauthorized Service

ID	Attack Name
US1	Unauthorized Service-A (External Server → Internal Server)
US2	Unauthorized Service-B (Internal Server → External Server)
US3	Unauthorized Service-C (Internal Server → Internal Server)
US4	Unauthorized Service-D (Internal Server → Field Control Device)
US5	Unauthorized Service-E (Field Control Device → Internal Server)
US6	Unauthorized Service-F (External Server → Field Control Device)
US7	Unauthorized Service-G (Field Control Device → External Server)
US8	Unauthorized Service-I (Field Control Device → Field Control Device)

○ Buffer Overflow

버퍼 오버플로우 공격은 대부분 소프트웨어 취약점을 이용한 공격으로 현재 많은 제어시스템 제품들이 이 공격에 노출되어 있다[3]. 대부분의 네트워크 패킷을 통한 버퍼 오버플로우 공격은 특정 통신 프로토콜이 제한한 최대 길이를 초과하거나, 길이 필드의 값과 다르게 설정된 패킷을 보냄으로써 이뤄진다. 본 논문에서는 공격에 이용한 프로토콜 종류 및 공격 방법(허용 최대 길이 초과, 길이 필드 값 불일치)에 따라 8가지 케이스로 분류하였다.

표 5. 버퍼 오버플로우 공격
Table 5. Attacks of Buffer Overflow

ID	Attack Name
BO1	Modbus Illegal Packet Size DoS
BO2	Modbus Incorrect Packet Length Field
BO3	DNP3 Illegal Packet Size DoS
BO4	DNP3 Incorrect Packet Length Field
BO5	MMS Incorrect TPKT Length Field
BO6	ICCP Incorrect TPKT Length Field
BO7	GOOSE Illegal Packet Size DoS
BO8	GOOSE Incorrect Packet Length Field

3) 최종 접속 일자 : 2013. 06. 25
http://www.digitalbond.com/blog/2012/09/06/100000-vulnerabilities/

○ Invalid Input Value

공격자는 입력 값에 대한 적합성 검사를 하지 않는 어플리케이션을 대상으로 비정상 입력 값을 통해 공격을 수행할 수 있다. 이 그룹의 세부 공격 유형으로 SQL Injection, XSS(Cross Site Scripting), Path Traversal 공격이 있다. Path Traversal 공격은 허가되지 않은 접근 주소를 통해 자원에 접근하는 것으로 웹 서버를 대상으로 비정상 url 주소를 입력하는 것이 대표적이다.

표 6. 비정상 입력 공격
Table 6. Attacks of Invalid Input Values

ID	Attack Name
IIV1	SQL Injection
IIV2	Cross-Site Scripting
IIV3	Path Traversal

○ Modbus Protocol Attack

Modbus 프로토콜은 인증 또는 암호화 메커니즘이 없기 때문에 제어 메시지에 대한 진본성 여부를 판단할 수 없다. 공격자는 Modbus 프로토콜에서 제공하는 다양한 function code들을 이용한 제어 메시지를 보냄으로써 공격 대상 시스템을 불법적으로 제어할 수 있다[4,10].

표 7. Modbus 프로토콜을 이용한 공격
Table 7. Attacks of Using Modbus Protocol

ID	Attack Name
MOD1	DoS-A (Brute Force)
MOD2	DoS-B (Restart Communication)
MOD3	DoS-C (Change ASCII Input Delimiter)
MOD4	DoS-D (Force Listen Only)
MOD5	DoS-E (Slave Device Busy Exception Code Delay)
MOD6	DoS-F (Acknowledge Exception Code Delay)
MOD7	Clear Counters Diagnostic Registers
MOD8	Read Device Identification
MOD9	Report Slave ID
MOD10	Unauthorized Read Request to a PLC
MOD11	Unauthorized Write Request to a PLC
MOD12	Points List Scan
MOD13	Function Code Scan
MOD14	Man-in-the-Middle Attack
MOD15	Replay Attack
MOD16	Non-Modbus Communication on TCP Port 502

○ DNP3 Protocol Attack

DNP3 프로토콜은 Modbus 프로토콜과 마찬가지로 인증, 암호화 메커니즘이 없기 때문에 수신된 제어 명령에 대한 진본성 여부를 판단할 수 없다[4]. 따라서 공격자는 가짜 제어 메시지를 통한 공격이 용이하다. [표 8]은 DNP3 프로토콜을 이용한 다양한 공격 방법들을 나타내고 있다[4,10].

표 8. DNP3 프로토콜을 이용한 공격
Table 8. Attacks of Using DNP3 Protocol

ID	Attack Name
DNP1	DoS-A (Pretend Slave Device Busy by setting DFC Flag)
DNP2	DoS-B (Link Layer FC 14-15 DoS)
DNP3	DoS-C (Message Reassembly DoS)
DNP4	Disable Unsolicited Responses
DNP5	Unsolicited Response Storm
DNP6	Cold Restart From Authorized Client
DNP7	Cold Restart From Unauthorized Client
DNP8	Unauthorized Read Request to a PLC
DNP9	Unauthorized Write Request to a PLC
DNP10	Unauthorized Miscellaneous Request to a PLC
DNP11	Stop Application
DNP12	Warm Restart
DNP13	Broadcast Request from an Authorized Client
DNP14	Broadcast Request from an Unauthorized Client
DNP15	Points List Scan
DNP16	Function Code Scan
DNP17	Non-DNP3 Communication on DNP3 Port

○ GOOSE Protocol Attack

GOOSE 프로토콜은 IEC 61850 통신 프로토콜 중 하나로 이더넷 기반으로 작동한다. GOOSE 프로토콜도 기본적으로는 메시지 인증 및 암호화를 제공하지 않기 때문에 중간자 공격이나 메시지 변조 등이 가능하다.

표 9. GOOSE 프로토콜을 이용한 공격
Table 9. Attacks of Using GOOSE Protocol

ID	Attack Name
GOOSE1	Man-in-the-Middle Attack
GOOSE2	Unauthorized Message Modification

4) IEEE 1815-2012 에서는 메시지 인증을 위한 Secure Authentication 기법 및 기밀성을 위한 IEC62351-3에서 정의된 TLS(Transport Layer Security) 사용을 정의하고 있다.

○ MMS Protocol Attack

MMS 프로토콜은 TCP/IP 스택 위에서 동작하며 HMI(Human Machine Interface) 등의 메인운영장치와 IED 간의 수직적 통신에서 일반적인 정보 수집, 파일 전송, 제어 명령 전달 등에 사용된다. IEC 61850에 정의된 기본 MMS 프로토콜은 인증 또는 암호화 메커니즘이 없기 때문에 메시지 변조 공격, 중간자 공격, 재전송 공격 등이 가능하다.

표 10. MMS 프로토콜을 이용한 공격
Table 10. Attacks of Using MMS Protocol

ID	Attack Name
MMS1	Man-in-the-Middle Attack
MMS2	Unauthorized Message Modification
MMS3	MMS Replay Attack

○ ICCP Protocol Attack

ICCP 프로토콜은 컨트롤 센터 간 통신에서 사용되는 프로토콜이다. 기존 몇몇 ICCP 서버 제품 중에서 TPKT(RFC 1006), COTP(ISO 8073) 레이어에서의 취약점이 발견된 바 있다[5]. ICCP 프로토콜 또한 기본적으로는 인증 및 암호화를 제공하지 않기 때문에 메시지 변조 공격 등에 취약하다.

표 11. ICCP 프로토콜을 이용한 공격
Table 11. Attacks of Using ICCP Protocol

ID	Attack Name
ICCP1	Man-in-the-Middle Attack
ICCP2	Unauthorized Message Modification
ICCP3	ICCP Replay Attack

○ TCP/IP - Spoofing

스푸핑(Spoofing) 공격은 MAC 주소 또는 IP 주소를 다른 주소로 바꿈으로써 송신 주소를 속이거나 통신 흐름을 조작하는데 이용된다. 이러한 공격은 공격자가 중간자 공격(Man-In-the-Middle Attack) 등 2차 공격을 하기 위한 사전 조건으로 사용되기도 한다. 대표적으로는 IP 스푸핑 공격과 ARP 스푸핑 공격이 있다.

5) CVE-2006-0059 (LiveData ICCP Server Heap Buffer Overflow Vulnerability)
CVE-2006-1178 (Tamarack MMSd Components Fail to Properly Handle Malformed Packets)
CVE-2005-4812 (Sisco OSI Stack Fails to Properly Validate Packets)

표 12. TCP/IP - 스푸핑 공격
Table 12. Attacks of Using TCP/IP Protocol - Spoofing

ID	Attack Name
SP1	IP Spoofing
SP2	ARP Spoofing

○ TCP/IP - Scanning

스캐닝(Scanning) 기법은 공격 대상 시스템의 활성 여부 또는 포트 상태를 알아내기 위한 공격으로 공격자가 사전 정보 습득을 위해 사용할 수 있다. 스캐닝 방법에 따라 [표 13]과 같이 9가지 세부 유형으로 분류할 수 있다.

표 13. TCP/IP - 스캐닝 공격
Table 13. Attacks of Using TCP/IP Protocol - Scanning

ID	Attack Name
SC1	ICMP Sweep
SC2	TCP Sweep
SC3	UDP Scan
SC4	TCP SYN Scan
SC5	TCP Half-open Scan
SC6	TCP ACK Scan
SC7	TCP NULL Scan
SC8	TCP Xmas Scan
SC9	TCP FIN Scan

○ TCP/IP - Others

본 논문에서 분류한 스푸핑 공격, 스캐닝 공격 외에 TCP/IP 프로토콜을 이용한 다른 공격 방법들은 기타 공격 방법으로 분류하였다. 여기에는 DNS Name Overflow, Teardrop, Windows Nuke, Slowloris, UDP 체크섬 에러를 이용한 공격, ICMP Unreachable Storm 등이 있다[3].

표 14. TCP/IP - 기타 공격(Other Attacks)
Table 14. Attacks of Using TCP/IP Protocol - Others

ID	Attack Name
OT1	DNS Name Overflow
OT2	Teardrop Attack
OT3	Windows Nuke
OT4	Slowloris Attack
OT5	UDP Checksum Error
OT6	ICMP Unreachable Storm

○ Flooding (Denial of Service)

Modbus on TCP/IP, DNP3 on TCP/IP, MMS, ICCP 등 최근 대부분의 제어시스템 통신 프로토콜이 TCP/IP 기반으로 동작함에 따라 기존 IT 환경에서 사용되던 flooding 공격 방법들이 그대로 적용될 수 있다. 한편 제어시스템 환경은 대역폭 및 시스템 자원이 한정적이기 때문에 소규모의 flooding 공격에도 가용성에 큰 영향을 받을 수 있다. 따라서 flooding 공격을 탐지하기 위한 임계점은 일반 IT 시스템 환경에서 보다 낮아져야 할 것이다.

표 15. 플루딩 공격
Table 15. Flooding Attacks

ID	Attack Name
FL1	Packet Flooding from Single Source
FL2	Packet Flooding from Multiple Source
FL3	Big Size Packet Flooding from Single Source
FL4	Big Size Packet Flooding from Multiple Source
FL5	Large Number of Session Creation
FL6	TCP SYN Flooding
FL7	UDP Flooding
FL8	ICMP Flooding
FL9	Snork Attack
FL10	TCP SYN/ACK Flooding
FL11	HTTP Get Flooding
FL12	ICMP Ping of Death
FL13	TCP Urgent Flooding
FL14	UDP Loopback

○ Fault

제어시스템에서 발생할 수 있는 오동작 유형은 다음 [표 16]과 같이 크게 8가지 케이스로 분류할 수 있다[7].

표 16. 오동작
Table 16. Fault

ID	Fault Name
FA1	System Shutdown
FA2	Service Stop
FA3	Packet Delay
FA4	Packet Loss
FA5	Bandwidth Overflow
FA6	Increasing Re-Transmission Packet
FA7	Increasing Collision Frame
FA8	Increasing Mal-formed Packet

Ⅳ. 화이트리스트 기반 이상 징후 탐지 기법

이 장에서는 3장에서 도출한 이상 징후 유형들을 탐지하기 위해 4계층으로 이루어진 화이트리스트를 제시하고, 이를 이용한 탐지 모델을 기술한다.

4.1. 제어시스템 네트워크 화이트리스트

본 논문에서 제시하는 화이트리스트 모델은 네트워크 계층(Network Layer), 프로토콜 명세 계층(Protocol Specification Layer), 제어 메시지 계층(Control Message Layer), 통계 계층(Static Layer)의 4계층으로 구분된다.

표 17. 제어시스템 화이트리스트
Table 17. Whitelists for SCADA

Layer	Whitelist Group
Network	Authorized Device
	Authorized Communication
	Authorized Service
Protocol Specification	Modbus Specification
	DNP3 Specification
	MMS/ICCP Specification
	GOOSE Specification
	DNS Specification
Control	Modbus Control Message
	DNP3 Control Message
	MMS Control Message
	ICCP Control Message
Statistic	Valid Throughput
	Valid Session Limit
	Valid Control Message Transmission
	Mal-formed Packet Limit
	Re-Transmission Packet Limit
	Collision Frame Limit

○ [Network Layer] Authorized Device
- 제어시스템 네트워크에 연결 가능한 장비 주소 (IP/MAC) 목록
- Tuple : IP address, MAC address
- 연관된 이상 징후 유형
  - Unauthorized Network Access : UA1-9
  - Spoofing : SP1-2

○ [Network Layer] Authorized Communication
- 통신이 허가된 두 노드의 주소 쌍 목록
- Tuple : Source IP, Destination IP
- 연관된 이상 징후 유형
  - Unauthorized Communication : UC1-3

○ [Network Layer] Authorized Service
- 특정 서비스 포트를 사용할 수 있는 서버/클라이언트 주소 쌍
- Tuple : Source IP, Destination IP, Port Number
- 연관된 이상 징후 유형
  - Unauthorized Service : US1-8

○ [Protocol Specification Layer] Modbus
- Modbus Specification
- Tuple : PDU 최대 길이 (256 bytes)
  Length 필드 위치 (offset : 4-5)
  Protocol Signature
  (offset : 0-1, signature : 0x0000)
- 연관된 이상 징후 유형
  - Buffer Overflow : BO1-2
  - Modbus Protocol Attack : MOD16

○ [Protocol Specification Layer] DNP3
- DNP Specification
- Tuple : Frame 최대 길이 (292 bytes)
  Length 필드 위치 (offset : 2)
  Protocol Signature
  (offset : 0-1, signature : 0x0564)
- 연관된 이상 징후 유형
  - Buffer Overflow : BO3-4
  - DNP3 Protocol Attack : DNP17

○ [Protocol Specification Layer] MMS / ICCP
- MMS/ICCP Specification
- Tuple : TPKT Length 필드 위치 (offset : 68-69)
- 연관된 이상 징후 유형
  - Buffer Overflow : BO5-6

○ [Protocol Specification Layer] GOOSE
- GOOSE Specification
- Tuple : GOOSE APDU 최대 길이 (1492 bytes)
  Length 필드 위치 (offset : 16-17)
  Protocol Signature
  (offset : 12-13, signature : 0x88b8)
- 연관된 이상 징후 유형
  - Buffer Overflow : BO7-8

○ [Protocol Specification Layer] DNS
- DNS Specification
- Tuple : DNS Name 필드 최대 길이(254 bytes)
- 연관된 이상 징후 유형
  - TCP/IP – Others : DNS Name Overflow

○ [Control Layer] Modbus
- Modbus를 사용하는 두 노드 간 사용할 수 있는 function code 집합
- Tuple : Source IP, Destination IP, Function Code Sets
- 연관된 이상 징후 유형
  - Modbus Protocol Attack : MOD1-15

○ [Control Layer] DNP3
- DNP3를 사용하는 두 노드 간 사용할 수 있는 function code 집합
- Tuple : Source IP, Destination IP, Function Code Sets
- 연관된 이상 징후 유형
  - DNP3 Protocol Attack : DNP1-16

○ [Control Layer] MMS
- MMS를 사용하는 두 노드 간 사용할 수 있는 메시지 타입 및 function 집합
- Tuple : Source IP, Destination IP, Message Type, Function Sets
- 연관된 이상 징후 유형
  - MMS Protocol Attack : MMS1-3

○ [Control Layer] ICCP
- ICCP를 사용하는 두 노드 간 사용할 수 있는 function 집합

- Tuple : Source IP, Destination IP, Function Sets
- 연관된 이상 징후 유형
  - ICCP Protocol Attack : ICCP1-3

○ [Statistic Layer] Valid Throughput
- 단위 시간 당 통신 패킷/바이트 허용 범위
- Tuple : 최대 전체 수신 패킷 수
  (Source IP, MAX pps)
  최대 전체 수신 바이트 수
  (Source IP, MAX bps)
  두 노드 간 최대 통신 패킷 수
  (Source IP, Destination IP, MAX pps)
  두 노드 간 최대 통신 바이트 수
  (Source IP, Destination IP, MAX bps)
  두 노드 간 최소 통신 패킷 수
  (Source IP, Destination IP, MIN pps)
  두 노드 간 최소 통신 바이트 수
  (Source IP, Destination IP, MIN bps)
- 연관된 이상 징후 유형
  - Flooding Attack : FL1-14
  - Fault : FA1-5

○ [Statistic Layer] Valid Session Limit
- 서비스 별 최대 유효 세션 수
- Tuple : IP address, Port, Session 수
- 연관된 이상 징후 유형
  - Flooding Attack : FL5
  - Fault : FA1-5

○ [Statistic Layer] Valid Control Message Transmission
- 단위 시간 당 두 노드 간 유효 명령 또는 상태 전달 수
- Tuple : Source IP, Destination IP, Port, message type, 단위 시간당 유효 개수 범위
- 연관된 이상 징후 유형
  - Any Protocol Attack : MOD1-15, DNP1-16, MMS1-3, ICCP1-3
  - Fault : FA1-5

○ [Statistic Layer] Mal-formed Packet Limit
- 네트워크 전체에서 단위 시간당 Mal-Formed 패킷의 허용 수
- Tuple : 단위 시간당 최소 허용 가능한 수
- 연관된 이상 징후 유형
  - Fault : FA8

○ [Statistic Layer] Re-Transmission Packet Limit
- 네트워크 전체에서 단위 시간당 재전송 패킷의 허용 수
- Tuple : 단위 시간당 최소 허용 가능한 수
- 연관된 이상 징후 유형
  - Fault : FA6

○ [Statistic Layer] Collision Frame Limit
- 네트워크 전체에서 단위 시간당 충돌 프레임 허용 수
- Tuple : 단위 시간당 최소 허용 가능한 수
- 연관된 이상 징후 유형
  - Fault : FA7

4.2. 화이트리스트 기반 탐지 모델

앞서 제시된 화이트리스트와 이상 징후 유형들을 통해 어떤 규칙을 위반하였을 때 어떤 이상 징후 유형과 연관되는지 [표 18]과 같이 도출할 수 있다.

표 18. 패킷 검사 기법 및 이상 징후 탐지
Table 18. Packet Inspection for Anomaly Detection

Inspection	Abnormally Cases
Validity of Device	Unauthorized Network Access ARP Spoofing IP Spoofing
Validity of Communication	Unauthorized Communication Scanning Attack
Validity of Service	Unauthorized Service Scanning Attack Flooding Attack
Validity of Protocol Specification	Buffer Overflow Invalid Input Value
Validity of Control Message	Modbus Protocol Attack DNP3 Protocol Attack MMS Protocol Attack ICCP Protocol Attack
Validity of Statistical Information	Flooding Attack Modbus Protocol Attack DNP3 Protocol Attack MMS Protocol Attack ICCP Protocol Attack

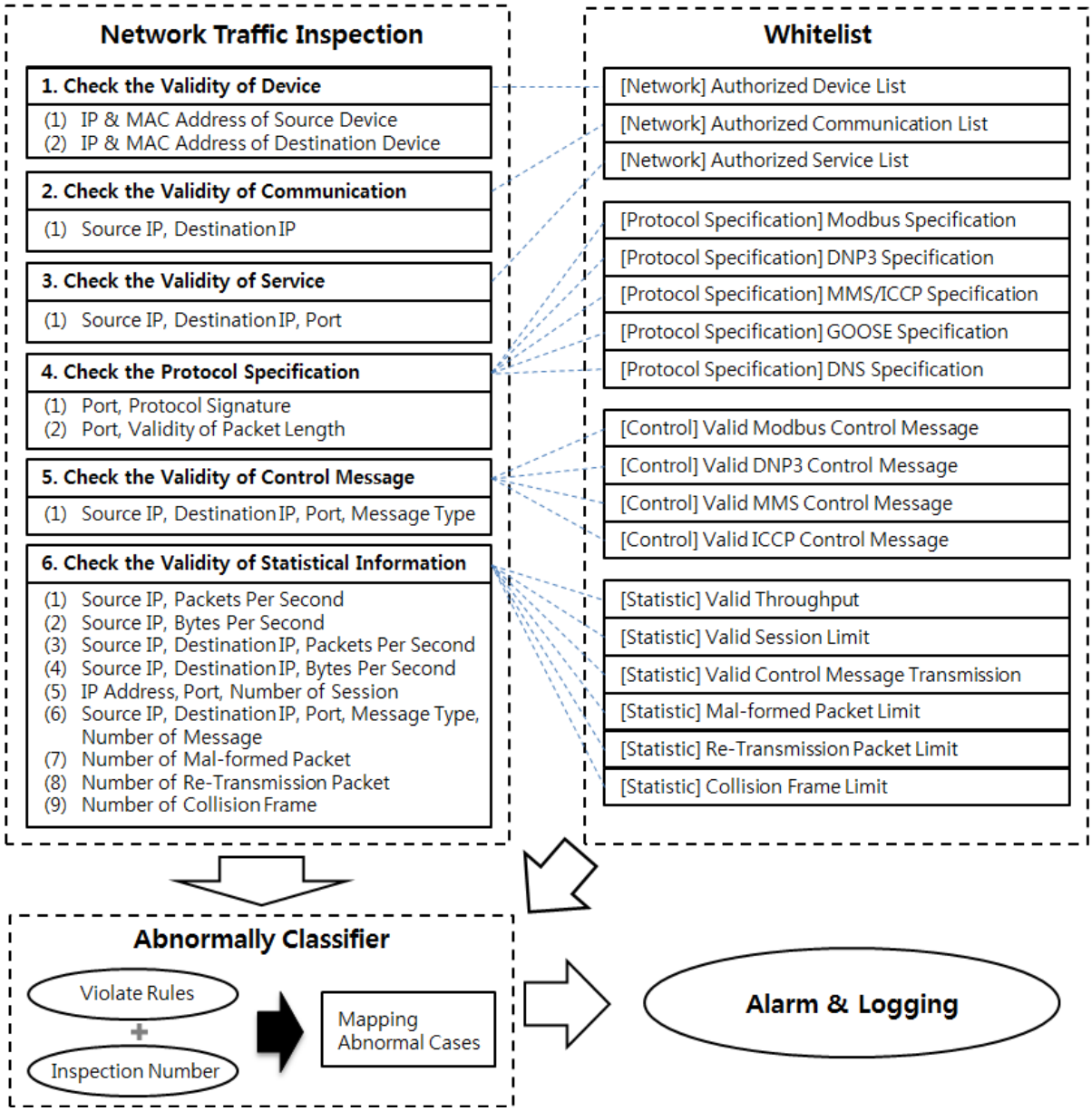

그림 3. 화이트리스트 기반 이상 징후 탐지 모델
Fig. 3. Whitelist based Anomaly Detection Model

[그림 3]은 본 논문에서 제시하는 화이트리스트 기반 이상 징후 탐지 모델을 나타내고 있다. Network Traffic Inspection 부분에서는 사전에 정의된 화이트리스트를 이용하여 개별 패킷 단위로 1~5번까지의 검사를 순차적으로 수행한다. 또한, 6번의 통계 정보 검사를 위해 단위 시간별 네트워크 트래픽 정보를 수집하고 이를 통해 6-(1)부터 6-(9)의 검사를 수행한다. Abnormally Classifier에서는 Network Traffic Inspection에서 위배 항목이 존재했던 검사 번호와 위배된 화이트리스트 규칙을 통해 3장에서 분류한 이상 징후 유형들 중 연관된 유형들을 추출하고 이에 대한 알람 및 로그 기록을 남긴다. 탐지된 이상 징후 유형에 대한 알람 및 로그 기록을 통해 보안 관리자에게 대응할 수 있는 정보를 제공할 수 있다.

V. 시나리오 기반 검증

본 논문에서 제시하는 화이트리스트 기반 이상 징후 탐지 모델을 검증하기 위해 제어시스템이 사용되는 대표적 도메인인 자동화 변전소에서의 2가지 이상 징후

탐지 시나리오를 제시한다.

○ Buffer Overflow Attack Using ICCP Protocol
- 전제조건 : 공격자는 외부 네트워크에 위치하며 방화벽을 우회하여 내부 제어 네트워크로의 접근이 가능하다.
- 공격대상 : 버퍼 오버플로우 취약점이 존재하는 ICCP 서버
- 공격목적 : 임의 코드 실행 또는 시스템 오동작 유발
- 공격방법 : 버퍼 오버플로우를 유발하기 위해 TPKT Length 필드에 명시된 길이와 일치하지 않는 비정상 패킷 전송
- 화이트리스트 위배 항목 :
  [Protocol Specification] MMS/ICCP Specification
- 탐지된 이상 징후 유형 : BO6

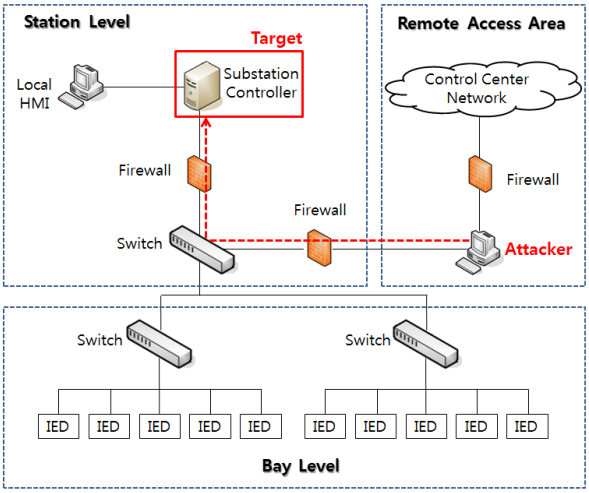

그림 4. 이상 징후 시나리오 1
Fig. 4. Anomaly Scenario 1

○ Unauthorized Write on Modbus Protocol
- 전제조건 : 공격자는 내부 네트워크에 위치하며 Local HMI에 대한 제어 권한을 가지고 있다.
- 공격대상 : Modbus 프로토콜을 사용하는 IED
- 공격목적 : IED 상태 변경
- 공격방법 : Modbus function code 0x05(Write Single Coil)로 설정된 패킷 전송
- 화이트리스트 위배 항목 :
  [Control] Valid MMS Control Message
  (Local HMI와 해당 IED 간에는 read 메시지 만 허용되는 화이트리스트 규칙 위배)
- 탐지된 이상 징후 유형 : MOD1-9, MOD11-15

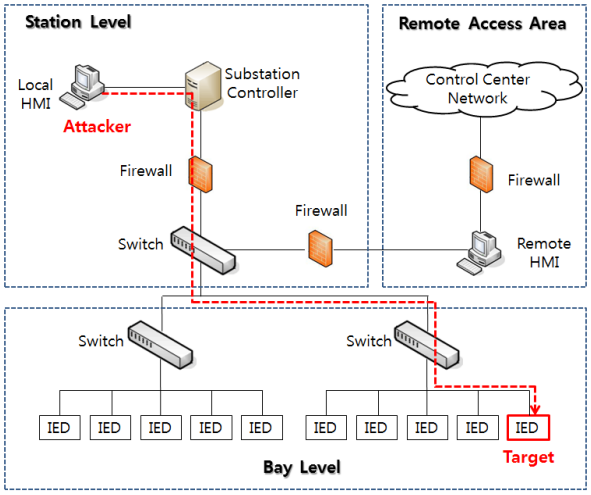

그림 5. 이상 징후 시나리오 2
Fig. 5. Anomaly Scenario 2

Ⅵ. 결 론

본 논문에서는 제어시스템을 대상으로 하는 고도화된 사이버 공격과 다양한 오동작 상황에 원활하게 대처하기 위해 화이트리스트 기반의 이상 징후 탐지 모델을 제시하였다. 제안하는 탐지 모델에서는 4계층의 화이트리스트를 통해 세분화된 검사를 수행할 수 있으며 기존 화이트리스트에서 기대하기 힘들었던 이상 징후 유형에 대한 정보를 제공할 수 있다. 향후에는 본 논문에서 제시한 이상 징후 유형을 좀 더 세분화·다양화할 필요가 있으며 사용되는 화이트리스트 또한 적용 프로토콜에 따라 구체화되어야 할 것이다.

References

[1] A. Ginter, "An analysis of Whitelisting security solutions and their applicability in control systems," in *SCADA Security Sci. Symp. (S4) 2010*, Miami, U.S.A., Jan. 2010.

[2] J. Yoon, W. Kim, and J. Seo, "Study on Technology Requirement using the Technological Trend of Security Products concerning Industrial Control System," *J. Korea Inst. Inform. Security Crytology*, vol. 22, no. 5, pp. 22-26, Aug. 2012.

[3] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. IEEE Int. Conf. Internet Things (iThings/CPSCom)*, pp. 308-388, Dalian, China,

Oct. 2011.

[4] I. N. Fovino, A. Coletta, and M. Masera, "Taxonomy of security solutions for the SCADA sector," *ESCoRTS, Deliverable D22*, Mar. 2010.

[5] D.-J. Kang, J.-J. Lee, S.-J. Kim, and J.-H. Park, "Analysis on cyber threats to SCADA systems," in *Proc. IEEE Transmission Distribution Conf. Expo.: Asia Pacific*, pp. 1-4, Seoul, Korea, Oct. 2009.

[6] M. Franz, "ICCP exposed: assessing the attack surface of the utility stack," in *SCADA Security Sci. Symp. (S4)*, Miami, U.S.A., Jan. 2007.

[7] Y. J. Won, "Fault detection, diagnosis, and prediction for IP-based industrial control networks," Ph.D. dissertation, Dept. Elect. Comput. Eng., Postech, Korea, Nov. 2009.

[8] U.S. Homeland Security, "Common cybersecurity vulnerabilities in industrial control," *Nat. Cyber Security Division, Control Syst. Security Program*, May 2011.

[9] IEC, "IEC 62351 part1 : communication network and system security - introduction to security issues," IEC TS 62351-1, May 2007.

[10] Digital Bond, *Quickdraw SCADA IDS*, Retrieved June, 26, 2013, from http://www.digitalbond.com/tools/quickdraw/.

[11] M. Jang, G. Lee, S. Kim, B.-G. Min, W.-N. Kim, and J. Seo, "Testing vulnerabilities of DNP3," *J. Security Eng.*, vol. 7, no. 1, Feb. 2010.

[12] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38-45, Aug. 2012.

유 형 욱 (Hyunguk Yoo)

2011년 8월 아주대학교 정보 및 컴퓨터공학부 졸업
2011년 9월~현재 아주대학교 컴퓨터공학과 석·박사 통합과정
<관심분야> 스마트그리드 보안, 디지털 포렌식, 이상탐지, 리눅스 및 안드로이드 보안

윤 정 한 (Jeong-Han Yun)

2001년 2월 KAIST 전산학과 졸업
2003년 2월 KAIST 전산학과 석사
2011년 2월 KAIST 전산학과 박사
2011년 3월~현재 ETRI 부설연구소 연구원
<관심분야> 프로그램 분석, 제어시스템 네트워크 침입탐지

손 태 식 (Taeshik Shon)

2000년 2월 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월 아주대학교 컴퓨터공학과 공학석사
2005년 8월 고려대학교 정보보호대학원 공학박사
2004년 2월~2005년 2월 University of Minnesota, Research Scholar
2005년 8월~2011년 2월 삼성전자 DMC 연구소 책임연구원
2011년 3월~현재 아주대학교 정보컴퓨터공학과 조교수
<관심분야> 스마트그리드 보안, 디지털 포렌식, 이상탐지, 시스템 및 네트워크 보안