*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.27, NO.1, Feb. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.1.25

# 비정상행위 탐지를 위한 시각화 기반 네트워크 포렌식

조 우 연,† 김 명 종, 박 근 호, 홍 만 표, 곽 진, 손 태 식‡
아주대학교

# Anomaly Detection Using Visualization-based Network Forensics

Woo-yeon Jo,† Myung-jong Kim, Keun-ho Park
Man-pyo Hong, Jin Kwak, Taeshik Shon‡
Ajou University

요 약

국가 주요 기반 시설을 포함하여 보안사고 발생 시 심각한 피해를 발생시킬 수 있는 산업 제어시스템의 특성에 의해 세계적으로 많은 보안 침해 사고가 발생하고 있다. 따라서 산업 제어시스템 네트워크에 오가는 트래픽은 감시되고, 분석되어 공격을 사전에 파악하거나 사고 이후 재빠른 대응을 수행할 수 있어야 한다. 본 논문에서는 제어시스템 프로토콜인 DNP3를 대상으로 모든 공격의 가능성을 갖는 트래픽들을 대상으로 합리적인 의심이 가능하도록 네트워크 포렌식 관점에서 시각화를 연구를 수행해 정상행위기반 룰을 정의하고 시각화 요구사항을 도출했다. 이를 기반으로 제어시스템 네트워크상에 캡처된 패킷 파일을 대상으로 DDoS와 같은 급작스런 네트워크 트래픽의 변화를 일으키는 경우 혹은 정상행위를 위반한 공격이 탐지 가능한 시각화 도구를 개발했고, 디지털본드 패킷과 같이 치명적인 공격이 포함된 네트워크상에서 성공적으로 비정상행위 탐지를 수행하였다.

ABSTRACT

Many security threats are occurring around the world due to the characteristics of industrial control systems that can cause serious damage in the event of a security incident including major national infrastructure. Therefore, the industrial control system network traffic should be analyzed so that it can identify the attack in advance or perform incident response after the accident. In this paper, we research the visualization technique as network forensics to enable reasonable suspicion of all possible attacks on DNP3 control system protocol, and define normal action based rules and derive visualization requirements. As a result, we developed a visualization tool that can detect sudden network traffic changes such as DDoS and attacks that contain anormal behavior from captured packet files on industrial control system network. The suspicious behavior in the industrial control system network can be found using visualization tool with Digital Bond packet.

**Keywords:** Industrial Control System, Industrial IoT, Visualization, Network Forensics, DNP3

## I. 서 론

산업제어시스템(Industrial Control System)은 전력, 철도, 가스 등 국가 주요 기반 시설들을 포함하여 다양한 도메인에서 확장되고 있는 추세로 그 크기도 소규모에서 국가 기반 시설까지 확대되고 있다. 단순 생산 및 조립라인에 그쳤던 과거의 공장 자동화와는 달리 현재 산업제어시스템은 감시 및 자동제어가 가능한 기술로 발전하여 사용자에게 편리성과 경제성을 제공하고 있다. 이에 따라 산업제어시스템 시장은 아직도 계속 증가하고 있는 추세이고, 더욱 다양한 분야에서도 산업제어시스템이 사용될 것으로 예상된다.

하지만 이러한 산업제어시스템 활용의 증가 추세

Received(01. 10. 2017), Accepted(01. 19. 2017)
† 주저자, dndusdndus12@gmail.com
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

와 함께 사이버 보안 침해 사고 발생도 증가하고 있다. 2010년 이란에서 발생한 스턱스넷(Stuxnet)을 시작으로 2015년 12월에 발생한 우크라이나 정전 사태까지 다양한 사고들이 발생하여, 제어시스템 보안 사고는 지금 어디에서나 발생가능하다는 경각심을 불러 일으켰다. 실제 ICS-CERT에 보고된 사이버 보안 사고는 매해 증가하고 있으며, 2015년 회계연도에 ICS-CERT에 보고된 북미 산업제어시스템을 대상으로 하는 보안 사고는 총 295건으로 2014년에 비해 20% 증가하였다. 보고된 사고들은 특정 도메인에서만 발생한 것이 아니라 Critical Manufacturing, Energy 등 다양한 산업제어시스템들에서 발생하였고, 공격 유형의 경우 알려지지 않은 경우가 가장 많았으며, 그 이후로 스피어 피싱, 네트워크 스캐닝 등의 공격들이 확인 되었다[1].

현재 국외의 경우, 이와 관련하여 ICS-CERT, ABB, SANS, Fire Eye 등에서 산업제어시스템에 디지털 포렌식 기술을 접목하여[2], 네트워크 로그 분석 등을 활용한 사후대응 절차를 마련하는 것에 대한 연구를 진행하고 있으며, SANS ICS Security Summit 등과 같은 학술회의에서 디지털 포렌식 기술을 산업제어시스템에 적용하는 방안에 대해 발표되는 등 제어시스템 보안을 위한 디지털 포렌식 기술 연구가 활성화되고 있는 추세이다.

그러나 현재까지 진행된 연구들은 아직 개념 정립 같은 연구 초기단계에 머물고 있으며, 국내 산업제어시스템의 특징을 반영하지 못하고 있기 때문에 국내 환경에 적합한 산업제어시스템 네트워크 포렌식에 대한 연구가 진행될 필요가 있다. 따라서 본 논문에서는 산업제어시스템 네트워크 프로토콜인 DNP3를 대상으로 시각화 연구를 통해 네트워크 포렌식 관점에서 제어시스템에 보안을 강화할 수 있는 플랫폼을 제안하고자 한다[3].

본 논문의 구성은 다음과 같다. 2장에서는 본 연구와 관련이 있는 제어시스템 대상 네트워크 포렌식 연구 및 시각화 연구들에 대해서 소개하고 본 논문의 시각화 대상이 되는 DNP3 프로토콜에 대해 다룬다. 3장에서는 DNP3 프로토콜의 정상행위를 분석하여 룰을 규정하고, 4장에서는 네트워크 트래픽과 규정된 룰에 대한 시각화 방안을 제시한다. 5장에서는 시각화 연구를 통해 개발된 도구로 파악할 수 있는 비정상행위 및 공격에 대해 소개하고, 6장에서 결론을 내린다.

## II. 관련연구

### 2.1 제어시스템 대상 네트워크 포렌식 연구

본 2.1장에서는 본 연구 목적과 유사한 제어시스템을 대상으로 진행된 네트워크 포렌식 연구들의 동향에 대해 다룬다.

#### 2.1.1 NETRESEC 社, 'NetworkMiner'[4]

NetworkMiner는 Network Forensic Analysis Tool(NFAT)로 2007년 NETRESEC에서 출시하였으며 가장 최신 버전은 2016년 2월에 출시된 2.0버전으로 1.4부터 제어시스템 프로토콜(IEC 60870-5-104) 파서를 지원하는 네트워크 포렌식 도구이다. NetworkMiner는 운영체제, 세션, 호스트 네임, 열려있는 포트 등등의 정보를 알려주는 네트워크 스니퍼 기능과 패킷 캡처하는 기능을 제공한다. 본 연구에서도 이와 같이 제어시스템 네트워크 프로토콜에만 국한되지 않고 하나의 네트워크 프로토콜로 취급하여 확장성을 확보하였다.

#### 2.1.2 FireEye, 'Industrial Control Systems Health Check'[5]

FireEye 社에서는  고객의 ICS 결함을 평가하고 보완해주는 서비스인 'Industrial control systems gap assessment'를 제공한다. 이 서비스를 통해 고객은 ICS 네트워크를 모니터링하여 산업 제어 시스템과 관련된 보안 위험에 대한 가시성을 확립하고, 분석할 수 있다. FireEye는 제어시스템을 평가하기 위해 특정 기기를 통해 네트워크 패킷을 캡처한 후 위험 분석과 위협 모델링을 통해 대응한다. 이처럼 특정 네트워크상에서 위협을 판별하기 위해서는 전문가의 도움과 그에 상응하는 비용을 필요로 하기 때문에 본 연구에서 제안하는 시각화 연구를 통해 제어시스템 네트워크를 관리하는 기관은 효과적으로 비용을 감축할 수 있을 것으로 기대한다.

#### 2.1.3 SCADA Systems: Challenges for Forensic Investigators[6]

2012년 미국 뉴올리언스 대학 및 ABB에서는 SCADA(Supervisory Control And Data

Acquisition)의 네트워크 환경에 디지털 포렌식 기법을 적용하기 위해 제어시스템의 네트워크 환경 및 특성을 분석하여 제어시스템 환경에 디지털 포렌식 기술을 적용하기 위해 고려해야하는 주요 요인을 도출하였다. 특히 제어시스템이 주 7일, 24시간 끊임없이 작동하는 특성을 고려한 라이브 포렌식 기법의 적용 필요성에 대해 강조하고 있으며, 이를 위해 사고 발생 시점을 기준으로 디지털 증거로서 인정받을 수 있는 유효기간 및 지속적으로 모니터링을 통해 수집해야하는 정보에 대해 언급하고 있다. 본 연구에서 제안하는 시각화 연구는 사고 발생 시점을 기준으로 패킷을 캡처한 이후 즉각적인 대응에 대한 해결책이 될 수 있도록 의심스러운 패킷에 대한 정보를 제공한다.

## 2.2 네트워크 포렌식 기반 시각화 연구

본 2.2장에서는 본 연구와 적용 분야는 다르지만, 시각화 연구의 접근 방법이 유사한 네트워크 포렌식 연구와 시각화 연구를 접목한 연구들에 대해 다룬다.

### 2.2.1 Multi-Dimensional Visualization for Network Forensic Analysis[7]

2011년 태국 King Mongkut's University of Technology North Bangkok에 소속된 연구실인 Faculty of Information Technology에서는 네트워크 환경에서 공격의 패턴을 분석하였다. 네트워크 시각화를 위해 Source IP 주소와 Destination IP 주소, 시간, 서비스를 분석하여 공격자를 효율적으로 찾을 수 있도록 가시화하였고, 악의가 없는 이벤트와 공격 이벤트의 패턴의 차이를 분석하였다. 해당 연구에서 분석한 것과 유사하게 본 연구에서는 프로토콜의 정상행위를 분석하고, 이후 정상행위와 비정상행위를 나누어 나타내었다.

### 2.2.2 Visualization Tool for Network Forensics Analysis Using an Intrusion Detection System CyberViz[8]

2009년 스리랑카 SLIIT(Sri Lanka Institute of Information Technology) 대학에 소속된 Department of Information Technology에서 네트워크상의 패킷들을 Winpcap으로 캡처하고 분석하였으며, 시각화 도구인 CyberViz를 연동하여 공격 패킷의 IP 주소와 공격 방식에 대해서 가시화하였다. 또한 연구에서는 CyberViz의 주요 기능인 네트워크 트래픽 가시화의 장점과 한계에 대해서 설명하고 있다. 해당 연구에서 활용한 Winpcap 형식의 파일은 널리 쓰이는 패킷 캡처 결과 파일(.pcap)로 본 연구에서도 같은 형식의 패킷 파일을 대상으로 하여 확장성과 실용성을 확보하였다.

### 2.2.3 University of Maryland, NetGrok[9]

미국의 메릴랜드 대학에서 만든 NetGrok은 처음으로 2008년에 배포되었고, 최신 배포는 2010년이다. 이 툴은 자바기반의 플랫폼으로 실시간으로 비주얼하게 트래픽으로 표시해준다. 이 툴의 주요 기능으로는 해당 Source IP 주소 및 필터링 옵션별로 가시화하여 네트워크를 한눈에 볼 수 있도록 트리맵 구조로 표현하며, pcap 파일로 저장하는 기능 등이 있다. 본 연구에서 제안하는 시각화 연구에서도 각 시각화 결과는 필터링 기능을 제공하여 프로토콜의 서비스별 혹은 정상행위 기반 룰 별로 정렬 가능하다.

## 2.3 DNP3 프로토콜 분석

본 연구에서는 산업제어시스템에 시각화를 기반으로 네트워크 포렌식을 적용시키기 위해 하나의 모범적인 예시로써 세계적으로 널리 쓰이는 프로토콜인 DNP3를 채택하여 연구를 진행하였다. 본 장에서는 시각화를 위해 먼저 DNP3 프로토콜의 패킷 구조를 분석하여 패킷이 갖는 정보 중 프로토콜 서비스를 나타내는 등 주요한 필드를 선별하였다.

### 2.3.1 DNP3 개요

DNP3 프로토콜은 Fig.1.과 같은 프로토콜 스택을 갖고 있으며, 본 논문에서 네트워크 포렌식 관점

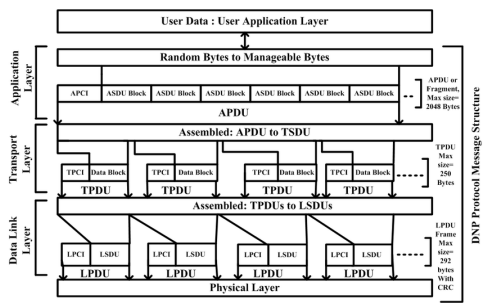


Fig. 1. Protocol Stack of DNP3

의 시각화 연구를 수행하기 위해 분석한 분야는 향후 다른 프로토콜로의 확장성을 확보하기 위해 프로토콜의 Fragment나 Frame 등이 모두 합쳐져 하나의 온전한 패킷을 나타낼 수 있는 Application Layer를 기준으로 한다.

### 2.3.2 DNP3 패킷 구조

본 시각화 연구에서 분석 대상으로 하는 Application 계층은 사용자 응용 프로그램과 직접 연결되는 계층으로 메시지를 받아서, ASDU (Application Server Data Unit)단위로 쪼개어 각 ASDU에 제어정보를 추가해서 APDU (Application Protocol Data Unit)을 생성한다. 아래 Fig.2.는 DNP3의 메시지 포맷과 그 변환 과정이 도식화되어있는 것을 볼 수 있다. 이 ASDU와 APDU가 본 논문에서 주로 다루는 Application 계층에서의 분석 대상이며, 그 안에 포함하고 있는 세부 필드에 대해서는 이후에 이어지는 장에서 다룬다.

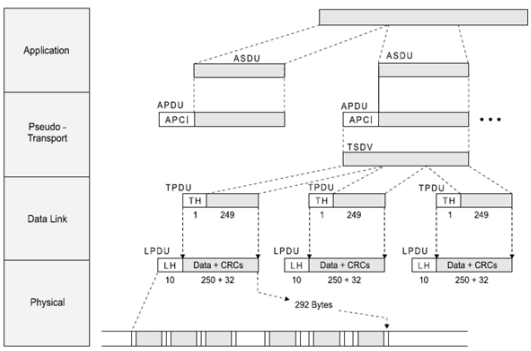


Fig. 2. DNP3 Message Format

### 2.3.3 DNP3 서비스

DNP3에는 다양한 서비스 제공을 위해 다수의 서비스를 제공하며, 각 서비스에 따른 프로토콜 규격이 표준에 정의되어 있다. 프로토콜에서 사용될 수 있는 서비스는 패킷의 FC(Function Code) 필드에 의해 구분되며, function의 종류는 총 36가지로 구성되어 있다. 36개 중 35개의 기능은 크게 Request와 Response 두 가지로 구분지어질 수 있으며, 이외에 Confirmation이 한 개 존재한다. Request 및 Confirmation은 0x80 이하의 영역에만 존재하며, 할당되지 않은 영역은 향후 만들어질 수 있는 Request 메시지를 위해 비워져있다. Response는 나머지 영역(0x80~0xFF)에 할당되어져 있으며 Request와 마찬가지로 할당되지 않은 영역은 예약되어있다.

본 연구에서는 DNP3 패킷의 FC(Function Code)를 기준으로 분류하여 Function 별 점유율을 분석하여 가장 많은 점유율을 차지하고 있는 Read Request 및 Response 서비스를 각 Request/Response 부분에서 대표적으로 정상행위 규정 대상으로 선별하고 상세 분석을 수행하였다. 이외에도 이벤트가 발생했을 경우 동작하는 Unsolicited Response와 전송 확인을 위해 쓰이는 Confirmation 서비스에 대해 정상행위 분석을 수행하였다.

## III. DNP3 정상행위 분석

### 3.1 DNP3 필드별 정상 범위 분석

본 장에서는 DNP3 패킷의 Function Code와 Object Group, Object Variation 등을 분석하여 정상행위에 판별하기 위해서 정상행위 규정에 필요한 APCI(Application protocol control information)의 AC(Application Control) 필드에 대해 보다 자세히 분석하였다. APCI의 구조는 Fig.2.와 같다.

APCI 필드는 마스터에서의 Request 메시지의 포맷과 아웃스테이션에서의 Response메시지의 포맷이 서로 다르지만, 위 그림에서 보듯이 AC(Application Control) 필드와 FC(Function Code) 필드는 서로 동일하다. AC 필드의 7번째, 6번째 비트는 각각 FIR, FIN 비트로 메세지가 Fragment 로 쪼개져 있는지 구별한다.

본 연구에서 분석 대상으로 하는 Application Layer에서 마스터와 아웃스테이션에서는 최대 송/수신 메시지의 크기가 2048bytes로 정해져있고, 최대 송/수신 메시지보다 많은 byte를 전송하기 위해서는 메시지를 Fragment로 나누어 여러 번 전송하여야 한다. 하지만 마스터에서 보내어지는 Request 메시지는 단일메세지로 보내는 것을 규정으로 하고 있다.

Table 1.을 보면 알 수 있듯이, FIR, FIN이 활성화 되었을 때에는 단일 메시지를 의미하고, FIR만 활성화되었을 때는 첫 Fragment, FIR, FIN이 비활성화 되었을 때에는 중간 Fragment, FIN만 활

Table 1. Combination of FIR, FIN bit

| FIR | FIN | Description |
|---|---|---|
| 1 | 1 | Single Message |
| 1 | 0 | First Fragment |
| 0 | 0 | Middle of Fragments |
| 0 | 1 | Last Fragment |

성화 되었을 때에는 마지막 Fragment를 의미한다.

위 Table 1.과 각 서비스가 갖는 특징에 따라 정상행위를 분석한 결과는 Table 2.와 같이 나타낼 수 있었다. Table 2.는 Function Code와 FIR , FIN의 관계를 보여준다. 마스터에서 보내어지는 요청(Request)메시지와 아웃스테이션에서 보내어지는 Confirm 서비스 항상 단일메세지로 전송되어야 하므로 FIR와 FIN이 활성화되어 전송된다. 아웃스테이션에서 보내어지는 Confirm 서비스를 제외한 다른 서비스는 메시지의 크기에 따라 FIR와 FIN의 활성화가 정해진다.

또한 APCI 이후 이어지는 ASDU 내의 Object 필드에 존재하는 Object Group/Object Variation 필드에 대한 정상행위를 규정하기 위해서 IEEE 1815-2012 표준을 참고하여 각 Object Group에 따른 Object Variation과 Function Code를 분석하였다. 예를 들어 바이너리 입력 포인트 값을 취득하거나 할당하는데 사용되는 (Object Group , Object Variation) 조합인 (0x01, 0x01~0x02)는 Function Code가 1(READ)나 22(ASSIGN_CLASS)가 쓰여야 한다. 하지만 모든 Object Group / Object Variation 그룹에 대해서 Function Code가 위의 예시와 같이 특정 값을 제한받는 것이 아니기 때문에 제어시스템 관리자는 시각화를 적용하기 전 사용자 정의된 변수들을 포함해 제어시스템이 갖는 제한된 조합에 대해 미리 시각화 담당자와 상의해야 한다.

아래 Fig.3은 표준에 예시로 제시되어 있는

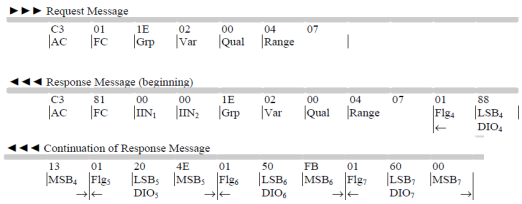


Fig. 3. DNP3 Example Packet

DNP3의 Read와 그에 대응하는 Response 패킷으로 위에서 분석한 패킷 필드들을 살펴볼 수 있다. 먼저 두 패킷은 각각 FC가 0x01, 0x81로 나타나 있어 Read와 Response임을 알 수 있다. Read의 Object Group를 0x1E, Object Variation을 0x02, Qualifier의 index는 0이고, Qualifier code가 0이므로 object는 Analog Input object 이고 index prefix는 없고, Range field에 8비트 Start 인덱스와 Stop 인덱스를 표시한다. 예시에서는 Start 인덱스를 4, Stop 인덱스를 7로 하여 Response 메시지는 요청메시지를 따라 4번에서 7번까지 인덱스의 데이터가 차례로 붙어서 오고, 데이터의 형태와 크기는 Object Group 0x1E, Object Variation 0x02에 따라 Analog Input objects에서 변형된 형태로 마스터에서 요청한 object를 아웃스테이션에서 마스터로 전송하게 된다. 이처럼 표준에는 각각의 FC와 더불어 다양한 종류의 Object Group과 Object Variation을 설명하기 때문에 정상적인 경우 어떠한 값을 갖게 되는지에 대해 분석 가능하며 분석된 정상행위를 토대로 다음 3.2장에서 룰로 규정하였다.

### 3.2 정상행위 기반 룰 규정

이전 2.3장에서 분석된 필드들이 가질 수 있는 값의 범위를 정상행위로 분류하고 각 필드의 관계에 따른 정상행위를 분석하여 정상행위를 토대로 룰을 규

Table 2. Function Code - FIR, FIN

| Function Code ( 1byte,0~255(Dec)) | FIR, FIN 상태 |
|---|---|
| 0 (Request, Response) | Only FIR = 1, FIN = 1 |
| 1~33 ( Request ) | Only FIR = 1, FIN = 1 |
| 34~128( Request-Reserved) | Only FIR = 1, FIN = 1 |
| 129~131 ( Response) | FIR = 0 or 1,FIN = 0 or 1 |
| 132~255 ( Response-Reserved) | FIR = 0 or 1,FIN = 0 or 1 |

Table 3. DNP3 protocol Rule based on Normal Behavior (SPR, TBR, DBR)

| Rule | | Description |
|---|---|---|
| Single Packet Based Rule | SPR 1 | Read Request Single Packet Based Rule Set |
| | SPR 1-1 | APCI Rule Set |
| | SPR 1-1-1 | Application Control Rule Set |
| | SPR 1-1-1-1 | Read Request AC FIR Field Test (Normal Value : 1) |
| | SPR 1-1-1-2 | Read Request AC FIN Field Test (Normal Value : 1) |
| | SPR 1-1-1-3 | Read Request AC CON Field Test (Normal Value : 1/0) |
| | SPR 1-1-1-4 | Read Request AC SEQ Field Test (Normal Value : 00~15) |
| | SPR 1-1-2 | Read Request FC Rule set |
| | SPR 1-1-2-1 | Read Request FC Field Test (Normal Value : 0x01) |
| | SPR 1-2 | Object Header Rule Set |
| | SPR 1-2-1 | Object Field Rule Set |
| | SPR 1-2-1-1 | Object Group Test |
| | SPR 1-2-1-2 | Object Variation Test |
| | SPR 1-2-2 | Object Qualifier Rule set |
| | SPR 1-2-2-1 | Object Prefix Test |
| | SPR 1-2-2-2 | Object Range Specifier Test |
| | SPR 1-2-3 | Object Range Rule Set |
| | SPR 1-2-3-1 | Object Range Test |
| Transaction Based Rule | TBR 1 | Read Request ↔ Response Transaction Rule |
| | TBR 1-1 | APCI Rule Set |
| | TBR 1-1-1 | Application Control Rule Set |
| | TBR 1-1-1-4 | Request, Response AC SEQ Field Test |
| | TBR 1-2 | Object Header Rule Set |
| | TBR 1-2-1 | Object Field Rule Set |
| | TBR 1-2-1-1 | Request, Response Object Group Test |
| | TBR 1-2-1-2 | Request, Response Object Variation Test |
| | TBR 1-2-2 | Object Qualifier Rule set |
| | TBR 1-2-2-1 | Request, Response Object Prefix Test |
| | TBR 1-2-2-2 | Request, Response Object Range specifier Test |
| | TBR 1-2-3 | Object Range Rule set |
| | TBR 1-2-3-1 | Request, Response Range |
| Digital Bond Rule | DBR 1 | Disable_Unsolicited Response(FC:0x15) Message Warning |
| | DBR 2 | Time Change Attempt Message Warning (Write(0x02), Object Group:50) |
| | DBR 3 | Stop Application(FC:0x12) Message Warning |
| | DBR 4 | Warm Restart(FC:0x0E) Message Warning |
| | DBR 5 | Cold Restart(FC:0x0D) Message Warning |

정한다. 본 연구에서는 정상행위 기반 룰뿐만 아니라 디지털 본드에서 규정한 Snort 룰을 자체적인 규격에 맞추어 변환해 추가하였다[10]. 아래는 DNP3 정상행위 기반 룰의 넘버링 방법이다.

*SPR(Single Packet based Rule): (Function Code) - (Specific Field) - (Detail Field) - (More Detail Field, if Needed)*

*TBR(Transaction Based Rule): (Transaction(Function) Type) - (Specific Field) - (Detail Field, if Needed)*

결론적으로 본 연구를 통해 DNP3의 시각화 대상 서비스인 Read에 대해 단일패킷 기반 룰(Single Packet Based Rule, 이하 SPR) 10가지와과 트랜잭션 기반 룰(Transaction Based Rule, 이하 TBR) 6가지를 개발할 수 있었고, 룰 넘버링 형식에

따라 작성한 내용은 Table 3.과 같다. 표에서는 각각의 필드에 따라 숫자가 부여되어 있으며, 예상되는 정상 값의 범위가 단순한 경우 표기하여 나타내고 있다.

Table 3.에는 본 연구를 통해 분석된 정상행위 기반 룰뿐만 아니라 디지털 본드에서 규정한 Snort 룰 또한 추가되어있다[10]. 디지털 본드에서 규정한 룰을 분석한 결과 본 연구에도 적용할 수 있는 룰이 존재함을 알아낼 수 있었으며, 해당 룰은 모두 서비스를 기반으로 경고를 주는 방식을 사용하고 있었다.

Table 3.의 각 룰은 Description에 서술된 내용을 통해 어떠한 필드를 기준으로 룰을 규정하였는지 파악할 수 있다. 각 룰의 *Specific Field*의 경우 APCI 필드와 Object Header 필드가 나올 수 있으며, Detail Field부터는 그 하위 필드를 나타낸다.

SPR(Single Packet based Rule)은 단일 패킷 기반 룰로 오직 한 개의 패킷만이 주어졌을 때 판단 가능한 필드를 기준으로 정상행위를 탐지하는 룰이다. SPR 1-1-1-1는 네 개의 단계에 걸쳐 나누어진 세부 필드를 살펴보는 룰임을 파악할 수 있다. SPR 1은 FC를 살펴보아 Read Request(0x01)인 경우에 한해 룰이 적용되는 것을 의미하며, SPR 1-1은 Read Request 패킷의 APCI 필드를 살펴볼 것을 의미한다. SPR 1-1-1은 APCI 필드 내에 있는 AC(Application Control) 필드를 살펴볼 것을 의미하며, SPR 1-1-1-1은 정상행위가 제한되는 FIR 필드를 살펴보는 것을 의미한다. 마찬가지로 SPR 1-1-1-#에 포함되는 SPR 1-1-1-1, 1-1-1-2, 1-1-1-3, 1-1-1-4는 모두 각각 AC 필드 내에 존재하는 FIR, FIN, CON, SEQ필드를 대상으로 정상행위 룰을 규정하고 있다.

TBR(Transaction Based Rule)은 SPR과 유사하게 룰의 번호가 부여되지만, 단일 패킷을 대상으로 하는 SPR과는 달리 서로 관련이 있는 두 개의 패킷을 살펴본 후 룰을 적용한다는 점에 차이가 있다. TBR 1은 Read Request와 그에 따른 Response 패킷을 대상으로 하며, TBR 1-1은 APCI 필드를 대상으로 TBR 1-1-1은 AC 필드를 대상으로 함을 의미한다. 여기까지는 SPR과 동일한 것으로 여겨질 수 있으나 TBR은 서로 영향을 주는 필드로 인해 제한적인 값을 정상행위로 지니게 되는 경우를 살펴보는 것이므로 모든 필드를 살펴보지 않고, 오직 제한이 생기는 필드만을 살펴보아 TBR 1-1-1-4만이 존재하게 된다. 이 필드는 AC필드 내에 존재하는 SEQ 필드로 반드시 Read Request와 Response가 동일한 값을 지녀야 하므로 패킷을 비교하여 정상행위 여부를 판단할 수 있다. TBR을 적용함에 있어 주의해야 할 점은 룰이 어겨진 비정상행위의 경우 Read Request와 Response 등의 두 상호관계에 놓인 패킷을 모두 살펴보고 어느쪽이 정말 잘못되었는지 파악해야 한다는 것이다.

DBR(Digital Based Rule)은 디지털 본드社의 Snort Rule을 기반으로 일부 룰만을 추출한 것으로 FC(Function Code)필드를 살펴 경고를 주기 위해 사용된다[10]. 이는 총 10여 가지가 넘는 디지털 본드 룰의 일부인 5가지에 불과하지만, 나머지 룰은 모두 허가받지 않은 IP로부터의 통신 혹은 특정 시간 내에 과도한 서비스의 사용 등으로 임의의 네트워크에서 적용하기 어려운 옵션이거나 시각화를 통해 훨씬 수월하게 파악 가능한 룰이므로 인용하지 않았다. DBR 룰은 모두 FC필드만을 기준으로 하기 때문에 SPR 및 TBR과는 달리 세부 필드가 존재하지 않는다.

## IV. 제안하는 DNP3 시각화 기반 포렌식

본 장에서는 분석한 제어시스템 네트워크 트래픽의 특성을 고려하여 시각화 대상을 선정하고, 시각화 방법에 대한 연구한 내용을 바탕으로 제어시스템 네트워크 포렌식을 위한 시각화 연구결과에 대해 논한다. 실증적인 연구 결과 도출을 위해 본 연구에서는 Digital Bond에서 자체적으로 Snort룰을 검사하기 위해 제작한 패킷을 사용하였다[10].

### 4.1 네트워크 트래픽 기반 시각화 대상 선정

산업 제어시스템 네트워크는 기기들의 동작과 측정값을 수집하고 특정 상황에 제어 명령을 내리는 것을 목표로 하고 있기 때문에 네트워크 트래픽이 단조롭다는 특성을 가진다. 주로 교환되는 정보들은 기기가 측정한 값, 기기의 상태정보 등이기 때문에 해당 제어시스템이 정상적으로 동작하고 있는 경우엔 큰 변화를 보이지 않는다. 따라서 네트워크에는 특정 서비스들만이 주로 사용되는 것으로 예상되며, 이는 패킷 분석 결과 확인되었을 뿐만 아니라 제어시스템 네트워크를 모니터링하는 관리자는 네트워크상의 서비스 분포에 대한 특성을 파악하고 있을 것이다. 이러한 특성에 따라 주로 사용되는 서비스가 아닌 다른 서비스들은 제어시스템이 정상적으로 동작하고 있지 않거나,

비정상적인 공격이 발생하였다고 판단 할 수 있음으로 본 연구진은 이에 착안하여 프로토콜에서 주로 사용되는 서비스(Function)들을 파악을 수행하고, 비정상적인 서비스들에 대한 시각화 방안에 대해 연구를 수행하였다.

DNP3 패킷에서는 항상 Read Request와 그에 따른 Response가 Polling 기능에 따라 대부분을 차지할 것으로 예상될 수 있으며, 각 변전소마다 쓰이는 서비스의 종류와 개수 등의 차이점이 존재하나 전체적인 트래픽의 흐름이 일정할 것으로 예상된다.

Read Request와 관련된 서비스를 제외하면, Confirm Request와 Unsolicited Response가 주로 사용되고 있다. Confirm 서비스의 경우 AC(Application Control) 필드 중 CON 비트가 1으로 설정된 경우 정상적으로 값을 받았다고 상대에게 확인 메시지를 보내는 것으로 Request에 대한 Response가 정상적으로 처리될 수 없는 경우 1로 설정한다. 또한 Unsolicited Response 메시지의 경우 상대의 정상 수신 여부를 파악하기 위해 CON 비트를 1로 설정하여 보낸다. 따라서 이 두 가지 CON 비트가 1로 설정된 경우에 Confirm 메시지를 보내 해당 메시지가 정상적으로 수신되었다는 것을 확인시킨다. 따라서 이 경우 중요한 서비스는 CON보다는 그 이전의 메시지임이 파악되었다. Unsolicited Response 메시지는 주기적인 모니터링에도 사용되지만, 특정 이벤트 발생에도 사용된다. 또한 Request에 대한 에러메시지에도 CON 비트를 1로 설정되기 때문에 이 두 가지 경우에는 사용자가 해당 메시지가 송신/수신된 시간을 파악하여 정밀 조사가 필요할 수 있다. 따라서 해당 서비스에 대해 추가 분석에 필요한 패킷 내용들에 대해 분석하였고 아래와 같은 기본적인 패킷에 대한 내용들을 도출하였다.

가) Time

사용된 서비스가 비정상적인 상황에서 발생한 것인지, 시스템의 타 로그 기록들과 비교하여 파악하기 위해 필요하다.

나) PacketID

공격이 의심되어 해당 패킷에 대해 정밀분석을 수행하고자 할 경우 시간 정보를 이용하여 패킷을 찾을 수도 있으나 동일 시간에 많은 패킷이 도달하는 경우에는 파악하기 힘들다는 문제점을 해소하기 위해 pcap 파일에서 제공되는 PacketID활용해야 한다.

다) IP Address

해당 패킷이 공격이라 판단되거나 의심되는 경우 해당 공격의 시작점을 파악하기 위해 Source IP를 관리자에게 제공해야 되며, 실제 공격이 수행된 경우 공격의 시작점 파악에 용이할 것으로 예상된다.

또한 해당 패킷이 공격이라고 판단되거나 의심되는 경우 공격 대상을 식별하기 위해 Destination IP를 관리자에게 제공해야하며, 공격 피해를 받은 대상에 대한 식별에 기여할 것으로 예상된다.

라) Function

어떠한 서비스를 사용하였는지 사용자에게 정보를 제공하여 이 패킷에 대한 추가분석 여부에 대한 판단을 가능하게 할 필요가 있다. Read와 Response를 제외한 다른 서비스들은 소량의 패킷만이 검출되었는데, 이 경우 일반적인 상황이 아닐 가능성이 존재하고 잘 사용되지 않는 서비스를 이용한 공격일 가능성을 배재할 수 없기 때문에 해당 서비스들의 시각화에 초점을 맞출 필요가 있다. 특히 패킷 분석 결과 발견한 Write 함수의 경우 기기에 명령을 내릴 때 사용되기도 하는 함수다.

마지막으로 패킷 분석 결과 발견된 Unknown Function의 경우 표준에서 정의되지 않은 서비스로 비정상적인 패킷이라는 것이 쉽게 확인되므로 패킷의 일부가 유실되어 잘못 해석된 것이 아닌 경우 해당 패킷은 의도적인 공격이라 간주될 수 있다. 하지만 단순 Unknown 서비스의 검출 여부를 통해 공격 여부를 판단하기는 어렵기 때문에 추가 분석을 위해 패킷의 주요 정보들을 제공할 필요가 있다.

본 장에서는 각 서비스들의 특징과 패킷 분석 결과 파악된 내용들을 토대로 각 서비스들의 사용 용도에 따라 해당 서비스를 악용한 공격에 대해 예상하고, 이를 토대로 시각화 도구에 필요한 사항들에 대해 분석하였다. 본 연구진은 이러한 분석한 요구사항들을 실제 도구에서 어떠한 형태로 시각화 할 것인지에 대해 논의를 수행하였다. 도출한 요구사항별 시각화 방법과 그 이유는 아래와 같다.

가) 프로토콜의 서비스 비율

DNP3 프로토콜의 서비스 비율을 나타내는 것은 비율을 나타낼 때 널리 사용되는 Pie Chart 형태로 나타내어 전체 대비 해당 서비스의 점유율이 얼마나

되는지를 한눈에 확인 가능하도록 표현하는 것이 바람직 할 것으로 사료된다. Pie Chart에서 아주 소규모로 나타나 그 비율을 그래프 안에 기입하기 어려운 경우 생각하도록 하여 전체적인 흐름에 대해서만 사용자가 판단할 수 있도록 하면 충분할 것으로 예상된다. 세부적인 정보를 원하는 경우 서비스별로 나타나는 그래프를 참고할 수 있도록 바로 연결시키는 것이 바람직 할 것으로 예상된다.

나) 사용되는 서비스의 종류

서비스의 종류에 대해 파악 가능해야한다는 요구사항은 위 서비스 비율을 통해 해결할 수 있다. 서비스 비율에서 아주 극소량 나타나 Pie Chart에 비율을 기입하기 어려운 경우 이를 생략하고 표현하도록 한다면 극소량의 패킷이 검출되는 서비스도 위에서 기술한 Pie Chart를 통해 서비스 정류에 대해 파악 가능하다.

다) 시간에 따른 트래픽 변화량

패킷이 시간에 따라 변화함을 보이기 위해 x축을 시간으로 설정하고 그 양의 변화를 보여주기 위해 y축을 패킷 수를 나타내는 막대그래프 형태로 표현하는 것이 바람직 할 것으로 판단된다. 좌측에서 우측으로 시간의 흐름을 나타내는 것은 일반적인 형태이며, 여기에 추가로 패킷의 양을 표현하기 위해 막대그래프와 꺾은선 그래프 형태가 사용될 수 있다. 꺾은선 그래프는 그 변화에 대해 민감하게 표현 할 수 있으나 막대그래프에 비해 여러 요소들을 비교하기에는 다소 부적합하다고 판단되어 막대그래프를 이용하여 이를 표현하였다.

라) 급격히 증감하는 특정 서비스 트래픽 변화량

앞의 요구사항과 동일한 형태인 막대그래프로 표현 가능할 것으로 예상된다. 하지만 이 경우는 서비스별로 표현하는 것이 주목적이기 때문에 각 서비스별로 해당되는 그래프를 하나씩 나타내야 한다.

마) 상세 패킷 정보 확인

Bar chart 형태로 나타낼 경우 한 개의 bar에 해당하는 패킷들에 대한 추가 정보를 제공하여 공격으로 의심될 경우 패킷의 상세한 정보를 확인할 수 있어야 한다. 제공해야 할 내용들은 총 5가지로 Table 형식을 활용하고자 하였다. 5가지의 정보를 함께 담는 Chart의 경우 복잡한 형태로 구성되기 때문에 사용자가 직관적으로 이해할 수 있고, 필요한 정보들에 대해 명확히 기재할 수 있는 Table을 사용하여 정보를 표현한다.

### 4.2 시각화를 통한 네트워크 프로토콜 정상행위 기반 비정상행위 탐지 방안

DNP3에 대한 정상행위 기반 룰 규정으로 SPR(Single Packet Based Rule) 10가지와 TBR(Transaction Based Rule) 기반 룰 6가지가 위반된 경우를 단위 시간에 따라 시각화하기 위한 방법들에 대해 고민하였고, 네트워크 포렌식 분석을 효과적으로 수행하기 위해서 가장 중요한 것은 시간의 흐름에 따라 룰에 위반된 비정상행위 패킷들을 분석할 수 있어야 한다고 결론지었다. 따라서 룰 시각화 연구에서는 포렌식 관점으로 시간에 흐름에 따라 단위 시간당 비정상 패킷(룰 위반 패킷)이 얼마나 나타나는 지에 대해서 사용자가 파악 가능하여야 하며, 비정상 패킷의 세부정보(pcap frame Number, IP Src Address, IP Dst Address, 위반한 룰 번호 등)를 효율적으로 분석이 가능하여야 한다.

구현을 목표로 하는 기능과 비슷한 예시를 찾아보자면, 패킷 분석에 주로 사용되는 상용 도구인 Wireshark가 Fig.4.와 같이 수집된 패킷들을 분석하여 파일을 단위 시간에 따라 모든 패킷(선 그래프)과 TCP errors 패킷(파란 막대그래프) 등으로 시각화하는 기능을 갖고 있다. Wireshark는 또한 추가적인 옵션으로 선 그래프 마우스 클릭 시와 마우스 오버 시에 해당 패킷에 대한 추가적인 정보(frame number 등)를 보여주는 것 등이 있다.

또한 그래프를 통해서 얻을 수 있는 트래픽에 대한 개략적인 흐름뿐만 아니라, 사용자의 선택에 따라 패킷이 지니는 정확한 값을 나타내고 추가적인 정보를 제공할 수 있기를 기대했다. 따라서 그려지는 그

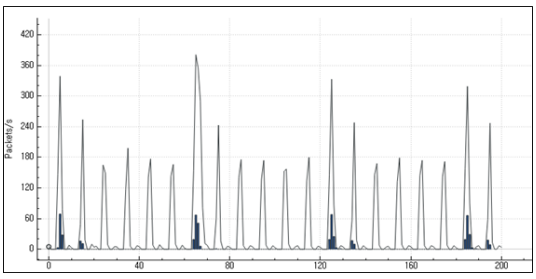


Fig. 4. Wireshark Packet Visualization

래프는 모두 룰마다 하나의 막대그래프를 가지며, 같은 시간대에 여러 가지의 룰을 위반하였을 경우에는 막대그래프를 쌓는 형식으로 시각화하여 사용자가 단위 시간당 룰을 위반한 패킷의 비율을 알 수 있게 설계하고자 하였다.

## V. 제어시스템 네트워크 시각화 방안 검증

본 장에서는 제어시스템 네트워크 포렌식을 위해 개발된 시각화 도구로 Digital Bond 社의 패킷을 이용해 산업 제어시스템 네트워크에 대해 얻은 유의미한 정보와 그에 따라 도구의 실효성을 검증한 내용을 다룬다.

도구는 아래 Fig.5.와 같은 방식으로 패킷 파일(.pcap)을 기반으로 파싱을 거쳐 D3.js 및 NVD3.js 등의 오픈소스 라이브러리를 사용해 웹 기반으로 그려지며, 본 논문에서는 결과적으로 그려지는 페이지만을 다룬다. 도구는 세 가지 뷰를 지니고 있는데, 전체 네트워크를 요약하는 뷰와 일반적인 트래픽 시각화를 수행하는 뷰 그리고 표준기반의 정상행위 룰에 대한 시각화 뷰이다. 사용된 제어시스템 네트워크 통신 트래픽은 Digital Bond社에서 공격을 포함하여 제작한 테스트 패킷 두 가지를 이용하였다.


Fig. 5. Visualization Tool Procedure

### 5.1 Main View 관점 검증 및 결과

기존에 설계한 Main view의 목적을 토대로 각 세부 뷰들의 개요를 나타내기 위해 Fig.6.과 같이 상단에 Traffic Overview를 나타내고 있으며, 하단에는 Rule Overview를 나타내고 있다. Main View에서 표현하는 내용은 Traffic Overview에서 Protocol Share, Function Share 두 가지의 Pie-Chart를 나타내며, Rule Overview에서 정상행위에 위반된 패킷의 흐름을 대략적으로 나타내는 Bar-Chart로 구성된다.

Traffic Overview의 Protocol Share는 네트워크에 존재하리라 예상되는 프로토콜(DNP3) 외에 존재하는 다른 프로토콜을 나타내어 네트워크상에 존

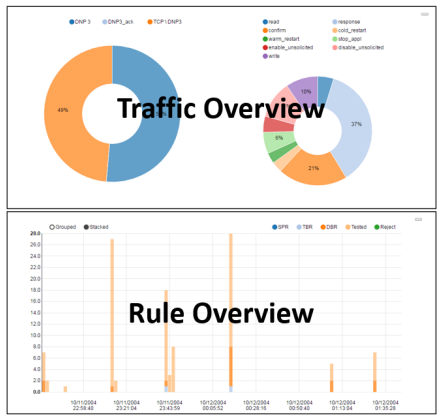


Fig. 6. Main View

재하지 않을 것으로 예상되는 패킷의 존재 유무와 비율을 파악할 수 있다. Function Share는 DNP3 프로토콜의 서비스들에 대한 비율을 나타낸 것으로 실제 패킷의 경우에도 네트워크상에 사용되는 서비스는 반복적으로 일정하게 사용되어질 것으로 예상돼 네트워크 관리자는 비정상적인 비율을 나타내는 서비스에 대해 공격을 의심할 수 있다. Rule Overview는 정상행위를 위반한 트래픽을 나타냄으로써 단 하나라도 존재한다면, 해당 패킷이 나타난 원인을 파악하고 공격인지의 여부를 판단하여 제어시스템의 보안을 강화해야 한다.

Main View에서 얻을 수 있었던 네트워크상에서의 비정상행위는 Digital Bond 社의 패킷에서 발견할 수 있었다. DNP3 프로토콜은 통상적으로 polling 기능으로 인해 Fig.7-(L)과 같이 Read request와 그에 따른 Response로 대부분의 트래픽을 이룰 것으로 예상된다. 하지만 Fig.7-(R)과 같이 다양한 서비스가 매우 자주 사용된 경우에 모니터링 관리자는 기존의 네트워크와 비교를 통해 비정

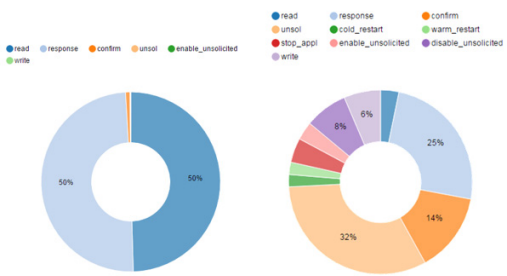


Fig. 7. DNP3 service share pie chart - (L)Real Substation Packet - (R) Digital Bond Packet

상행위가 일어났음을 짐작할 수 있었다. 이는 자주 쓰이지 않는 서비스가 모종의 원인으로 인해 과도하게 사용되었거나, 자주 쓰여야 할 서비스가 사용되지 못한다는 것을 의미한다. 이러한 상황에서 관리자는 합리적인 의심을 통해 자세한 분석에 대한 필요성을 느낄 것이며, 아래 Traffic View와 Rule View에서 제공하는 다양한 기능들을 활용한 분석과 조사를 통해 그 원인을 파악할 수 있다.

### 5.2 Traffic View 관점 검증 및 결과

시각화 연구에서 도출된 설계를 토대로 개발한 결과 Traffic View에 Fig.8.과 같이 두 종류의 그래프를 그렸다. 그래프는 Traffic Stream과 Traffic Detail을 나타내며, Traffic Stream은 Stacked Area Chart 형식을 채용하였으며 3 가지의 레이아웃을 통해 전체 트래픽 흐름 정보를 사용자에게 효과적으로 전달하고자 하였다. 하단 그래프인 Traffic Detail은 Multi-Bar Chart 형식을 채용하여 각각의 서비스를 따로 선택하여 나타내도록 변경할 수 있다. 아래 Fig.9.는 패킷을 나타낸 Traffic View


Fig. 8. Traffic View

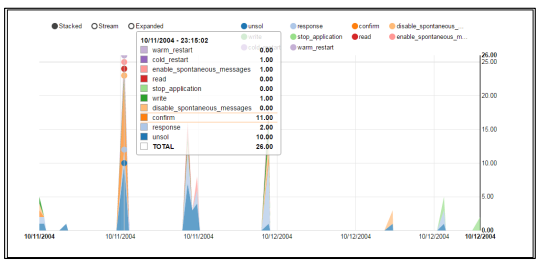

Fig. 9. Traffic Stream - Stacked mode

를 캡처한 것으로 캡처 시작 이후 2번에 걸쳐 큰 트래픽 흐름이 존재했던 모습을 확인할 수 있다.

또한 아래 Traffic Stream의 Stream 레이아웃을 적용한 Fig.10.을 통해 서비스의 비율이 각 트래픽마다 다른 종류의 서비스가 주로 사용되었음을 쉽게 파악할 수 있다. 이러한 변화들이 모두 공격을 의미한다고 할 수는 없으나 공격이 발생할 경우 대부분 비정상적인 트래픽을 동반할 것으로 예상된다. Fig.11.과 Fig.12.를 통해 의심스러운 행위를 포착하여 시각화 도구를 통한 네트워크 포렌식으로 원인을 신속히 파악하고 사건 발생 시점을 규정함으로써 관리자의 즉각적인 대응을 가능하게 할 수 있다.

관리자는 비정상적인 트래픽의 흐름을 위에서와 같이 파악한 이후 Traffic Detail 그래프를 통해 보다 상세한 정보를 획득 가능하다. Traffic Detail의 각 Bar는 의 경우 클릭 시 팝업을 통해 패킷의 세부 정보를 나타낼 수 있도록 하였다. 팝업 시 패킷의 상세 정보는 아래 Fig.11, 12.와 같이 나타난다. 아래에 나타나 있는 패킷은 Unsolicited Response를 허용/비허용하는 서비스인 Disable/Enable Spontaneous Message를 정렬한 모습이다. Fig.11에서는 비허용(Disable) 메세지가 한 시점에 동일한 메시지가 세 번 호출되었으며 세 메시지 모두 source IP와 destination IP

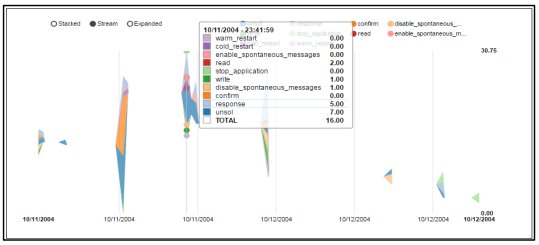

Fig. 10. Traffic Stream - Stream mode

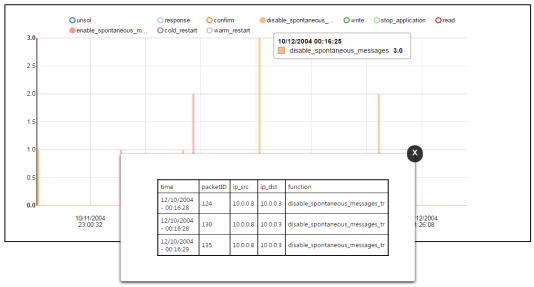

Fig. 11. Traffic Detail - Popup

가 동일하게 작성되었음을 확인 가능하다. 해당 서비스는 빈번히 사용되지 않는 만큼 관리자가 직접 명령을 내린 것이 아니라면, 시스템이 비효율적인 동작을 수행하고 있거나 공격자가 공격을 위해 준비과정을 거치는 것으로 충분히 의심 가능한 상황이 될 수 있다. 따라서 관리자는 서비스의 사용이 정당한 권한을 거쳐 이루어졌는지 확인해야 한다.

반대로 Fig.12.는 Popup을 통해 허용(Enable) 메시지를 보내는 경우를 보이고 있으며, Fig.11.과 흡사하게 동일한 IP를 가진 Source와 Destination을 나타내고 있다. 만약 공격자가 공격을 수행하고 있다면 정상적인 기기를 대상으로 Unsolicited 메시지를 금지해 서비스를 중단시키고, 감염된 기기를 허용시켜 최종적으로 DDoS 공격을 감행하고 있을 것으로 추측할 수 있다.

이처럼 Traffic View를 통해서 관리자는 비정상적인 서비스의 트래픽 증감 혹은 사용되지 않거나 명령하지 않은 서비스의 사용을 확인하고, 비정상행위를 감지한 이후 popup 기능을 활용하여 상세한 분석을 수행할 수 있다.

| time | packetID | ip_src | ip_dst | function |
|---|---|---|---|---|
| 11/10/2004 - 23:46:53 | 109 | 10.0.0.9 | 10.0.0.3 | enable_spontaneous_messages_tr |
| 11/10/2004 - 23:47:00 | 113 | 10.0.0.9 | 10.0.0.3 | enable_spontaneous_messages_tr |

Fig. 12. Popup View(Detail Information)

### 5.3 Rule View 관점 검증 및 결과

Rule View는 SPR(Single Packet Based Rule) Chart, TBR(Transaction Based Rule) Chart, DBR(Digital Bond Rule) Chart로 구성된다. 본 연구에서 검증 대상으로 사용하는 패킷은 디지털 본드에서 제작한 패킷으로 공격이 포함되어 룰을 위반하는 패킷이 다수 존재할 것으로 예상되며, 그 결과 예상과 동일하게 디지털 본드의 Snort 룰을 기반으로 한 DBR에 위반된 경우가 다수 존재하는 것을 확인했으며, 자체적인 룰에도 일부 패킷이 검출되는 발견하였다.

룰을 위반하는 경우 정상적으로 검출되는지에 대해서는 아래 Fig.13.에서 나타내는 대로 Digital Bond 社 Packet을 토대로 테스트하여 표준을 위반한 경우 혹은 Digital Bond에서 규정한 경우에 대해 정상적으로 검출되는 것을 확인할 수 있었다.

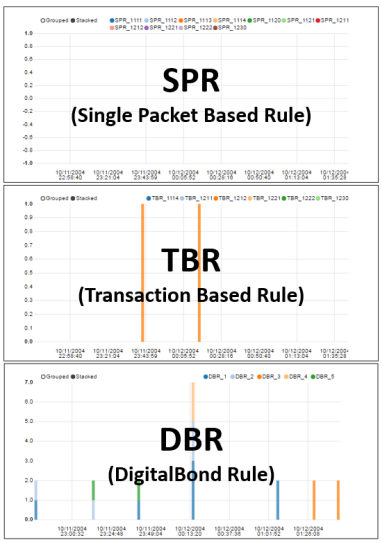


Fig. 13. Rule View

이처럼 Digital Bond 패킷에서 비정상행위가 Rule을 위반하여 네트워크상에 존재함을 확인할 수 있었고, 자체적으로 정상행위를 기반으로 정의한 룰을 통해서도 비정상행위 감지가 가능함을 보였다. 비정상행위 탐지의 경우 시각화 도구를 사용하는 관리자는 Rule View에서 단 하나의 패킷도 놓치지 않고 면밀히 살펴 제어시스템의 보안에 완벽을 기해야 한다.

## VI. 결 론

본 논문은 산업제어시스템에서 추세의 변화에 따른 기술 선도와 확장성을 유지한 채 가용성 보장하고 사이버 공격에 대한 즉각적인 대응에 효과적으로 도움을 주는 시각화 기반 산업제어시스템 네트워크 포렌식 연구를 수행하였다. 그 과정에서 현재 국내 제어시스템 네트워크 프로토콜로 쓰이고 있는 DNP3에 대해 분석을 수행하였으며, 분석 결과를 토대로 프로토콜의 정상행위를 파악하고 룰을 규정하였다. 또한 해외 보안업체인 Digital Bond 社가 정의한 DNP3 Snort Rule 일부를 룰에 추가함으로써 완성도 높은 룰을 규정하였다. 규정된 룰은 SPR 10가지, TBR 6가지, DBR 5가지로 총 21가지로 DNP3 프로토콜을 사용하는 네트워크에 가해질 수 있는 다양한 공격을 탐지할 수 있다.

네트워크 포렌식 관점에서 이루어진 시각화 방안 연구는 규정된 룰뿐만 아니라 기존 프로토콜의 주요

필드를 살펴 시각화 대상을 선정하고, 시각화 도구의 설계에 필요한 요구사항을 도출하였다. 이로써 앞서 규정한 룰뿐만 아니라 제어시스템 네트워크 트래픽과 패킷의 주요 정보를 사용자에게 제공하여 비전문가도 설계된 시각화 도구를 통해 이상 징후를 판별할 수 있으며, 주요 패킷 정보를 통해 원인을 파악하고 조사를 진행할 수 있다. 비전문가가 이처럼 도구를 통해 네트워크 포렌식을 진행할 수 있게 된다면 관련 기관에서는 보안사고 발생 시 즉각적인 대응을 적은 비용을 통해 수행할 수 있으며, 보안 전문가 또한 상세히 분석된 보고 내용을 통해 공격의 유무와 사고 발생원인 파악을 신속히 진행할 수 있을 것으로 기대한다.

본 연구에서 사용한 패킷은 Digital Bond 社에서 제공한 패킷으로 향후 진행될 연구에서는 실제 제어시스템을 대상으로 패킷을 캡처하여 실효성을 증명한 후 트래픽과 정상행위 룰을 통해 파악할 수 있는 비정상행위의 종류를 자세히 분류하여 규정할 필요가 있다.

## References


[1] ICS-CERT, "ICS-CERT Monitor November-December 2015", Nov, 2016.

[2] ICS Security Summit, "What's the DFIRence for ICS?", https://www.sans.org/event-downloads/42402/agenda.pdf, p.4, Feb. 2016

[3] IEEE Power and Energy Society, IEEE Standard for Electric Power Systems Communications.Distributed Network Protocol (DNP3), 2012

[4] NETRESEC, NetworkMiner, http://www.netresec.com/?page=NetworkMiner, 2016.

[5] FireEye, Industrial Control Systems Health Check, https://www.fireeye.com/services/mandiant-industrial-control-system-gap-assessment.html, 2016.

[6] Ahmed, Irfan, et al. "SCADA systems: Challenges for forensic investigators." Computer vol. 45, pp.44-51, Dec. 2012.

[7] Promrit, Nuttachot, et al. "Multi-dimensional visualization for network forensic analysis." Networked Computing (INC), 2011 The 7th International Conference on. IEEE, Sept. 2011.

[8] Abeyrathne, K. B., et al. "Visualization Tool for Network Forensics Analysis Using an Intrusion Detection System CyberViZ.", vol. 3, Dec. 2009.

[9] van Riel, Jean-Pierre, and Barry Irwin. "InetVis, a visual tool for network telescope traffic analysis." Proceedings of the 4th international conference on Computer graphics, virtual reality, visualisation and interaction in Africa. ACM, pp. 85-89, Jan. 2006.

[10] Blue, Ryan, et al. "Visualizing real-time network resource usage." Visualization for Computer Security. Springer Berlin Heidelberg, vol. 5210, pp. 119-135, Sept. 2008.

[11] Digital Bond, Download the PCAP files to test the Quickdraw Signatures, http://www.digitalbond.com/tools/quickdraw/download/, 2016


## 〈저 자 소 개〉


조 우 연(Woo-yeon Jo) 학생회원
2015년: 아주대학교 정보컴퓨터공학과 졸업(학사)
2015년~현재: 아주대학교 컴퓨터공학과 재학(통합)
〈관심분야〉 디지털 포렌식, 네트워크 시각화, 제어시스템 보안, IoT 보안, 개인정보보호

김 명 종(Myung-jong Kim) 학생회원
2016년: 아주대학교 정보컴퓨터공학과 졸업(학사)
2016년~현재: 아주대학교 컴퓨터공학과 재학(석사)
〈관심분야〉 IoT 보안, 제어시스템 보안, 네트워크 시각화

박 근 호(Keun-ho Park) 학생회원
2016년: 아주대학교 정보컴퓨터공학과 졸업(학사)
2016년~현재: 아주대학교 컴퓨터공학과 재학(석사)
〈관심분야〉 금융 보안, 제어시스템 보안

홍 만 표(Man-pyo Hong) 종신회원
1981년: 서울대학교 계산통계학 졸업(학사)
1983년: 서울대학교 계산통계학 졸업(석사)
1991년: 서울대학교 병렬처리 전공 졸업(박사)
1985~현재: 아주대학교 사이버보안학과 교수
〈관심분야〉 정보보호, 악성코드, DDoS, 스마트그리드 보안, 클라우드 보안

곽 진(Jin Kwak) 종신회원
2000년 성균관대학교 졸업(학사)
2003년 성균관대학교 졸업(석사)
2006년 성균관대학교 졸업(박사)
2007~2015년 순천향대학교 정보보호학과 교수
2015년~현재 아주대학교 사이버보안학과 교수
〈관심분야〉 암호프로토콜, 개인정보보호, 정보보호제품평가, 클라우드 보안, 자동차 보안

손 태 식(Taeshik Shon) 종신회원
2000년: 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년: 아주대학교 정보통신전문대학원 졸업(석사)
2005년: 고려대학교 정보보호대학원 졸업(박사)
2004년~2005년: University of Minnesota 방문연구원
2005년~2011년: 삼성전자 통신/DMC 연구소 책임연구원
2011년~현재: 아주대학교 정보통신대학 사이버보안학과 부교수
2017년~현재: Illinois Institute of Technology 방문교수
〈관심분야〉 산업제어시스템 보안, 비정상행위탐지, 디지털 포렌식