Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1455

산업제어시스템에서의 MITM 공격을 방어하기 위해 개선된 프로토콜

고 무 성,† 오 상 교, 이 경 호‡
고려대학교 정보보호대학원

Advanced protocol against MITM attacks in Industrial Control System

Moo-seong Ko,† Sang-kyo Oh, Kyung-ho Lee‡
Korea University, Graduate School of Information Security

요 약

국가 주요기반 시설인 산업제어시스템이 스턱스넷과 같은 악성 웜에 감염되는 경우 국가적 재난이 발생할 수 있다. 따라서 산업제어시스템에 대한 정보보호 연구는 활발히 진행되고 있다. 하지만, 대부분의 산업제어시스템 방어는 이러한 위협으로부터 시스템을 보호하기 위한 네트워크에서의 침입 탐지에 초점이 맞춰져 있다. 현재 국내에서 연구되고 있는 기존의 방법은 네트워크 트래픽을 모니터링하고 변칙 패턴을 검출하는데 효과적이나 MITM 기법을 이용한 정상 패턴과 동일한 공격 유형은 탐지하기 어렵다. 본 연구에서는 실제 산업제어시스템 현장의 데이터를 수집하여 PROFINET/DCP 프로토콜과 취약점을 분석하고 인증데이터 필드를 추가하여 MITM 공격을 방어 가능한 개선된 프로토콜을 제시 하며 이에 대한 적용 가능성을 확인한다. 본 논문에서 제시하는 개선된 프로토콜을 실 적용 시 MITM 공격으로 인해 발생할 수 있는 국가적 재난 발생을 방지할 수 있다.

ABSTRACT

If the industrial control system is infected by malicious worm such as Stuxnet, national disaster could be caused inevitably. Therefore, most of the industrial control system defence is focused on intrusion detection in network to protect against these threats. Conventional method is effective to monitor network traffic and detect anomalous patterns, but normal traffic pattern attacks using MITM technique are difficult to be detected. This study analyzes the PROFINET/DCP protocol and weaknesses with the data collected in real industrial control system. And add the authentication data field to secure the protocol, find out the applicability. Improved protocol may prevent the national disaster and defend against MITM attacks.

Keywords: SCADA, ICS, Protocol, DNPSec, PROFINET, DCP, MITM

I. 서 론

국가기반시설의 필수 구성요소인 제어시스템은 계측 및 제어, 상태 감시 및 관리를 위해 다양한 산업 분야에서 폭 넓게 사용되고 있다(1). 이러한 제어시스템은 SCADA(Supervisory Control And Data Acquisition System), 분산 제어시스템인 DCS(Distributed Control System), PLC (Programmable Logic Controller) 및 센서 등 다양한 구성요소 및 유형들로 이루어져 있다. 제어시스템은 일반적으로 인터넷망과 분리되어 운영되고 통신을 위한 전용 프로토콜이 사용되어 왔다. 따라서 제어시스템을 대상으로 한 사이버 위협의 가능성이 없다고 인식되어 왔으나 2010년 Stuxnet(2)이 발견되면서 급격한 변화가 이루어졌다. 이후 Duqu, Flame, Gauss, Mahdi, Shamoon, SkyWiper

Received(09. 03. 2015), Modified(10. 28. 2015), Accepted(11. 03. 2015)
† 주저자, mooseong@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

등 새로운 제어시스템 대상 악성코드가 지속적으로 발견되면서 제어시스템에서 침입을 탐지하기 위한 기술에 대하여 많은 연구가 있었다.

트래픽 패턴 분석(3)(4)(16), 산업제어시스템 로그 분석(5), 모니터링 기반 모델(6)과 같은 비정상 행위 탐지 기법은 산업현장에 위치한 개별기기의 보호(7)에 다섯 가지 제약이 있다. 첫째, 기존의 시스템 및 소프트웨어를 변경하는 것은 불가능하다. 둘째, 보안관리 시스템을 산업제어 하드웨어 및 소프트웨어에 설치하기 어렵다. 셋째, 산업제어시스템 내부에서 발생하는 네트워크 트래픽은 탐지 및 차단에서 벗어날 수 있다. 넷째, 산업제어시스템을 종료시키거나 재부팅하는 것이 불가능하다. 다섯째, 추가적인 트래픽이 생성되지 않아야 한다.

트래픽을 모니터링하고 비정상 패턴을 검출하는 방법은 네트워크 트래픽이 정상 패턴인지의 여부에 집중한다. 따라서 DoS나 DDoS와 같은 Flooding 공격과 같은 비정상 행위를 탐지하는 데에는 적합하나 공격자가 스푸핑을 통해 정상 패턴의 패킷을 전송하는 경우에는 탐지가 불가능하다.

본 연구에서는 PROFINET/DCP 프로토콜의 실제 데이터를 기반으로 PROFINET/DCP 프로토콜 구조와 보안 취약성을 분석하고 이를 보완하기 위한 방법을 고려함으로써 프로토콜 개선방안을 제안하고, 실효성을 입증한다. 이는 기존 통신환경에서 프로토콜의 취약성을 최소화하기 위한 방안으로 향후 발생할 수 있는 보안 위협을 방지할 수 있다.

본 연구의 2장에서는 국내 A 발전기관의 실 데이터를 기반으로 PROFINET/DCP 프로토콜의 구조와 통신 패턴을 분석한다. 3장에서는 발생할 수 있는 위협을 식별하고 가능한 공격 방식을 살펴본다. 4장에서는 PROFINET/DCP 프로토콜의 취약성을 보완하기 위한 방안 도출을 위해 DNPSec 프로토콜을 분석한다. 5장에서는 취약성을 보완한 프로토콜을 제안하고 도입 가능성을 측정한다. 마지막으로 6장에서는 제안한 프로토콜의 성능과 실효성을 측정 및 분석한다.

II. 사전연구

PROFINET은 지멘스사(Siemens)와 Profibus 사용자 조직(PNO)이 공동 개발하고 산업제어시스템에서 사용되는 산업용 이더넷 환경 표준으로 일곱 가지의 프로토콜로 나뉜다(8). PROFINET/IO와 CBA는 각각 독립적으로 각각의 역할을 수행하며 PROFINET/DCP, MRP, MRRT, PTCP, RT는 PROFINET/IO와 CBA를 지원하기 위한 프로토콜이다(11).

DCP 프로토콜은 PROFINET/IO 프로토콜을 사용하는 시스템의 디바이스가 지닌 장치명, IP 주소, MAC 주소 등과 같은 설정을 식별하고 설정하기 위한 프로토콜이다(12)(13). DCP의 프로토콜 구조는 Table 1.과 같다(10).

PROFINET은 디바이스 액세스 포인트에 IP 주소를 동적으로 할당하기 위해 DHCP(Dynamic Host Configuration Protocol)를 지원하며 PROFINET/IO 디바이스는 주소 변환을 위해 DCP(Dynamic Configuration Protocol)를 지원한다(14). 따라서 DHCP와 DCP가 동일한 목적을 위해 상호 보완적인 관계에 있다. 서비스 ID는 Set, Get, Identify와 같이 통신의 목적을 식별하기 위한 필드이며 Service Type은 Request, Response와 같은 통신의 종류를 식별하기 위한 필드이다(9). 또, Xid는 트렌젝션을 식별하기 위한 필드이고 NameOfStation은 패킷이 생성된 디바이스의 이름 필드이다(9)(15).

실제 산업제어시스템 네트워크의 PROFINET 통신 과정에서 PROFINET/DCP 프로토콜은 일정한 패턴을 갖는다. 각각의 디바이스는 다른 디바이스에 주기적으로 REQUEST 패킷을 전송하는데 모 발전소의 실제 산업제어시스템으로부터 수집하여 분석한 패턴은 Fig.1.과 같다.

이러한 REQUEST 패킷의 반복은 적절한 인증과 무결성 검증이 이루어지지 않을 경우 공격자가 악의적인 목적으로 패킷을 조작하여 시스템의 붕괴를 초래할 수 있다.

Table 1. PROFINET/DCP Protocol Stack

PROFINET/DCP
FrameID
ServiceID
Service Type
Xid
NameOfStation
Response Delay
DCP Data Length
Data Block

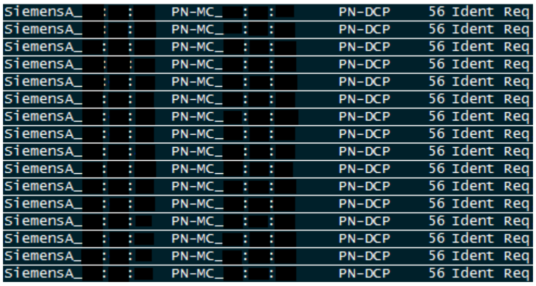

Fig. 1. PROFINET/DCP Communication Pattern

두 번째 패턴은 각각의 디바이스에 의해 변화하는 Xid 값이다. Xid 값은 각 디바이스별로 다르게 변하는데 Fig.2.와 Fig.3.은 디바이스 1 및 디바이스 2에 의해 Xid값이 변화하는 모습을 나타내고 있다(23).

앞서 분석한 바와 같이 PROFINET/DCP 프로토콜의 실제 통신은 일정 패턴을 지니고 있어 공격자가 해당 패턴을 이용하여 MITM 공격을 수행하기가 용이하다. 따라서 PROFINET/DCP 프로토콜 구조 및 패킷 데이터를 분석한 결과에 따라 가능한 실제 공격을 식별할 수 있다.

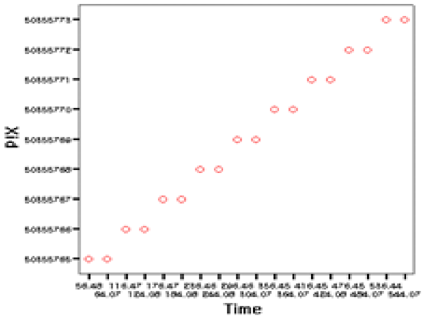

Fig. 2. Change of Xid(Device 1)

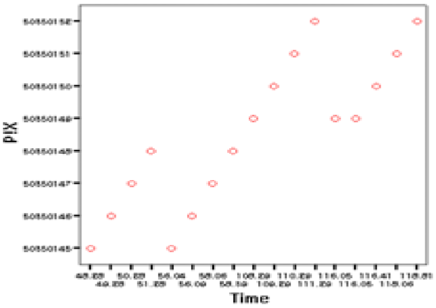

Fig. 3. Change of Xid(Device 2)

III. 공격 시나리오

3장에서는 PROFINET/DCP의 특징을 이용한 공격으로 산업제어시스템에 장애가 발생할 수 있는 세 가지 사례를 소개한다.

3.1 Packet Modification

공격자는 스푸핑과 같은 공격방법을 통해 네트워크 상 통신 패킷의 내용을 변조, 재전송할 수 있다. 디바이스 1이 디바이스 2를 식별하거나 구성값을 확인, 변경하고자 할 때 DCP Request 패킷을 전송한다. 이를 수신한 디바이스 2는 DCP Response 패킷을 전송하는데, 공격자는 MITM 공격을 활용하여 디바이스 2가 전송한 DCP Response 패킷을 가로채 패킷의 내용을 변조하여 재송신 하는 공격이 가능하다.

공격자는 일반적인 DCP Response 패킷을 일부만 수정하여 재전송하므로 비정상 행위 기반 탐지 시스템이 탐지하기 어렵다. 변조된 패킷을 수신한 디바이스 1은 잘못된 정보를 기초로 동작하게 되고, 이는 곧 제어시스템 전체에 치명적인 피해를 입힐 수 있게 된다.

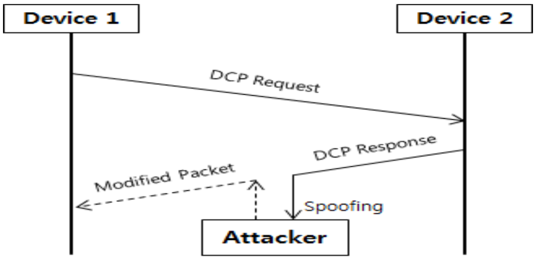

Fig. 4. Packet Modification Attack Process

3.2 Packet Sniffing

Request와 Response는 디바이스와 디바이스 간 통신에 사용되는데 공격자는 이러한 디바이스 간 통신을 훔쳐보고 장치명을 식별할 수 있다. 공격자는 타겟 디바이스를 선정하고 해당 디바이스의 Response 패킷을 Fig.5.와 같이 스니핑하여 디바이스 2에서 보내지는 모든 Response 패킷을 도청할 수 있다. 공격자는 도청한 패킷이 포함한 정보를 토대로 산업제어시스템의 구성을 유추할 수 있으며

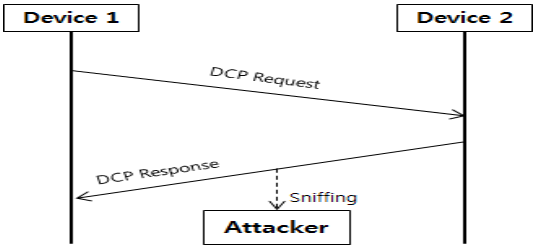

Fig. 5. Packet Sniffing Attack Process

유추한 정보는 추가적인 공격에 활용될 가능성이 높다.

3.3 Packet Fabrication

공격자는 디바이스 1에서 전송한 DCP Request 패킷과 동일한 형태의 위조 패킷을 작성, 디바이스 2로 전송할 수 있다. 위조된 DCP Request 패킷을 수신한 디바이스 2는 요청 패킷을 처리하고 DCP Response 패킷을 디바이스 1로 전송한다. 공격자는 정상 패턴과 동일한 형태의 위조 패킷에 디바이스 2의 구성값을 바꾸거나 동작을 정지하도록 명령을 담을 수 있다. 이는 곧 제어시스템의 붕괴를 초래할 수 있는 강력한 공격이 된다.

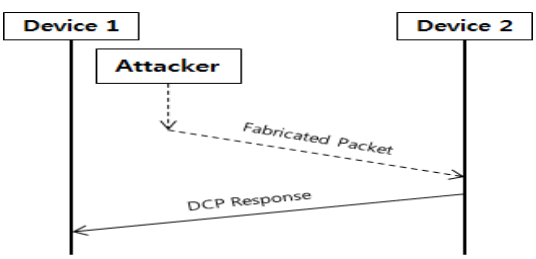

Fig. 6. Packet Fabrication Attack Process

IV. DNPSec 프로토콜 보안 기법 분석

DNPSec 인증 및 무결성 프레임워크는 DNP3 프로토콜을 보완하기 위해 개발된 것으로 원본 프레임을 확인할 수 있으며 전송된 프레임은 수신된 프레임과 동일하다는 것을 보장한다. 또한 프레임 전송 과정 중에 네트워크 헤더가 변경되지 않았음을 보장하고 인증 데이터 필드를 통해 리플레이 공격과 MITM 공격을 방어하기 위한 보호기능을 제공한다(17). 뿐만 아니라 DNPSec은 DNP3 프로토콜 기반 메시지의 기밀성, 무결성, 인증 보장을 제공하며 통신 성능 저하를 최소화시키기 위해 제안된 프로토콜로 MITM 공격에 취약한 DNP3 프로토콜을 효과적으로 보완했다.

DNPSec은 Fig.7.과 같이 다섯 개의 필드인 New LH 헤더, Key Sequence Number, Original LH 헤더, Payload Data, Authentication Data로 구성된다. New LH 헤더 필드는 목적지 주소 정보를 포함하고 있다.

Key Sequence Number 필드는 마스터가 메시지를 전송할 때마다 하나씩 증가하는 카운터 값을 가진다. 마스터는 메시지를 전송할 때마다 카운터를 증가시키고 Key Sequence Number 필드를 갱신한다. 이런 종류의 기능은 마스터와 슬레이브 간 연결이 항상 열려있는 경우에도 새로운 세션 키를 확립할 수 있게 한다. 또한 마스터와 슬레이브가 일정 시간 이상 동일한 세션 키를 사용하는 경우에 새로운 세션 키를 생성하도록 보안 정책을 적용할 수 있게 한다.

Original LH 헤더 필드와 Payload Data 필드는 암호화를 통해 보호된다. Authentication Data 필드는 Key Sequence Number 필드, Original LH 헤더 필드, Payload Data 필드의 값들을 통해 계산하여 산출된 Integrity Check Value(ICV) 값을 포함하고 있다. ICV는 특정 메시지 인증 알고리즘(MAC)을 통해 무결성 서비스를 제공한다(17)(24).

DNPSec은 인증 데이터 필드를 두고 ICV값을 기록하여 인증을 제공하며 Transport 계층의 CRC를 활용하여 무결성을 보장하고 있다. 그러나 앞서 살펴본 바와 같이 PROFINET/DCP 프로토콜은 디바이스의 설정을 설정, 확인, 디바이스를 식별하는 매우 중요한 역할을 수행함에도 불구하고 인증 데이터를 통한 방어기법이 적용되어 있지 않아 공격자가 MITM 공격을 수행하기 용이하다(25)(26). 따라서 같은 문제를 안고 있던 DNP3 프로토콜을 개선한

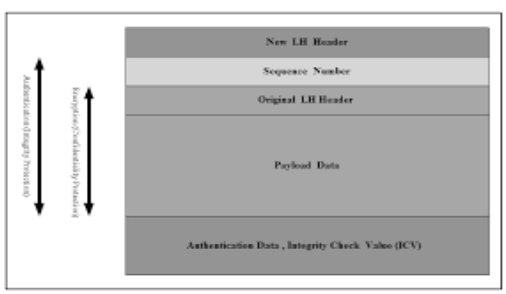

Fig. 7. DNPSec Protocol Stack

DNPSec의 문제점 보완 방법을 통해 PROFINET/DCP 프로토콜이 MITM 공격을 방어할 수 있도록 개선하여야 한다.

V. PROFINET/DCP 프로토콜 개선 방안

PROFINET/DCP 프로토콜은 인증과정이 부재하기 때문에 MITM 공격에 취약하다. 따라서 DCP 프로토콜 헤더에 인증 데이터 필드를 추가한 인증과정이 필요하다. 제안하는 개선된 프로토콜인 DCPSec은 기존의 DCP 프로토콜 스택에 Authentication Data Block 필드를 추가하고 암호화된 인증 데이터를 적재하여 인증과정을 추가한 것으로 기존 DCP 프로토콜이 지니고 있던 보안상 문제점을 해결하였다.

Table 2.와 같이 DCPSec에는 기존의 프로토콜 구조에 Authentication Data Block 필드를 추가하여 무결성과 인증을 보장한다. Data Block 필드는 디바이스의 설정과 관련한 정보를 포함하거나 설정을 위한 정보를 포함하고 있다. 인증 데이터는 Data Block의 정보를 DES 혹은 Triple DES를 이용해 암호화한다. 이렇게 생성된 암호화 데이터는 인증 데이터 필드에 적재되고 패킷을 수신한 디바이스에서 복호화 및 데이터 검증 작업을 통해 인증과 패킷 무결성을 확인할 수 있다. DCPSec의 전체적인 동작 프로세스는 다음과 Fig.8.과 같다.

프로토콜의 통신과정에 암호화 및 복호화가 추가되며 패킷의 데이터 블락의 크기가 증가하므로 전송 신뢰성 문제와 전송지연이 발생할 수 있다. 산업제어시스템에서 전송 신뢰성과 응답시간은 매우 중요한 요소이다(19)(20)(21). 전송 신뢰성은 데이터 링크 계층에서 전송 오류를 검출하는 비 암호 메커니즘인 순환 중복 코드(CRC)를 통해 제공되고 인증과정의

Table 2. PROFINET/DCPSec Protocol Stack

PROFINET/DCPSec
FrameID
ServiceID
Service Type
Xid
NameOfStation
Response Delay
DCP Data Length
Data Block
Authentication Data Block

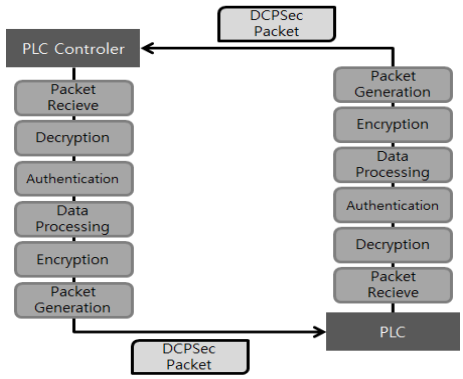

Fig.8. PROFINET/DCPSec Protocol communication process

추가로 인한 전송지연의 발생은 불가피하다. 그러나 여러 암호화 및 복호화와 키 설정 시간, 전송시간의 성능에 대한 연구에 따르면 네트워크 통신 기술, 종단 시스템에서의 처리능력, 암호화 알고리즘에 기초하여 인증 데이터의 추가로 인한 응답시간 지연이 매우 작음을 알 수 있다.

Kim 과 Montgomery의 연구(18)에서는 대규모 VPN 환경에서의 IPSec과 IKE가 갖는 성능과 동작 특징을 시험했다. Kim 과 Montgomery의 연구에서 밝힌 성능 정보에 의하면 DCPSec의 구현과 적용으로 인해 발생하는 지연은 매우 작은 수준에 그친다. 암호화와 복호화는 산업제어시스템에서의 응답시간에 최소한의 영향을 미친다. 연구에 의한 DES 및 Triple DES의 암호화와 복호화의 성능은 다음 Table 3.과 같다.

상기 성능 정보에 기초하여 디바이스 간 데이터 전송 지연 시간 측정을 위해 메시지는 292byte, Triple DES는 112비트 키 선택 알고리즘을 갖는다고 가정한다. 이때 네트워크 대역폭은 1.5Mbps이며 동작 속도는 kbit/s 단위로 설정하고 암호화 키와 복호화 키는 사전에 배포한다고 가정한다. 메시지를 전송하기 위한 전체 지연 시간은 암호화 및 복호

Table 3. Encryption and Decryption Performance

Operation	DES	3-DES
Encryption Speed (kbit/s)	10508 kbit/s	4178 kbit/s
Decryption Speed (kbit/s)	10519 kbit/s	4173 kbit/s

화 속도, 암·복호화 키 선정, 전송 시간의 합이다.

$$\text{Total DT} = \text{ES} + \text{DS} + \text{EK} + \text{DK} + \text{TT}$$

암호화 속도가 4178 Kbit/s 일 때 암호화에 소요되는 시간은 0.00007초이며 복호화 속도가 4173 Kbit/s 일 때 복호화에 소요되는 시간은 0.00007초이다. 1.5Mbps 대역폭 환경에서 292byte 메시지의 전송에는 0.0002초가 소요된다. 따라서 인증 데이터를 생성, 전송하며 발생하는 전송지연은 전체 0.00034 초이다.

변전소 자동화 설계를 위한 국제 표준인 IEC 61850에서는 전송시간을 4ms 이하로 규정하고 있다(22). PROFINET/DCP 패킷의 평균 간격은 3 μs이며 인증 데이터 필드를 도입, 인증과정을 추가하여 발생하는 전송 지연은 0.034ms로 IEC 61850에서 요구하는 허용 전송시간을 크게 밑돈다. 암호화는 상위계층인 Application 계층에서 이루어지고, 전송은 패킷의 출발지점에서부터 측정한 것을 고려하여도 상당히 작은 수치임에는 틀림없다.

Table 4. Time for operations

Operation	Performance	Time
Encryption	4178 kbit/s	.00007 s
Decryption	4173 kbit/s	.00007 s
Transmission	1.5 Mbit/s	.0002 s

VI. PROFINET/DCPSec 성능 검증

본 장에서는 PROFINET/DCPSec 프로토콜에 대한 유효성 및 성능 검증을 진행한다. 유효성은 스니핑 공격을 기반으로 확인하며 암호화 및 복호화 기술은 C 언어로 개발되고 구현은 Linux 운영체제(Xubuntu 12.04 LTS)에서 이루어졌다. PLC 시뮬레이터는 Conpot 허니팟을 사용하여 지멘스사 S200 모듈과 동일하게 시뮬레이션 하였으며 시뮬레이션 환경 구조는 다음 Fig.9.와 같다.

PROFINET/DCP 프로토콜의 전송에는 지멘스사에서 제공하는 PROFINET Commander 도구를 활용하여 암호화 과정 없이 Data Block 필드에 292byte의 메시지를 포함하여 다음 Fig.10.과 같이 전송했다.

PROFINET 프로토콜의 최소 간격이 3μs일 때

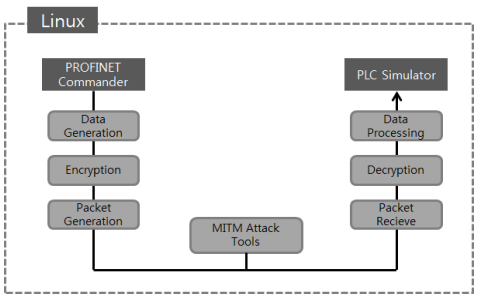

Fig. 9. PROFINET/DCPSec Sumulation Structure

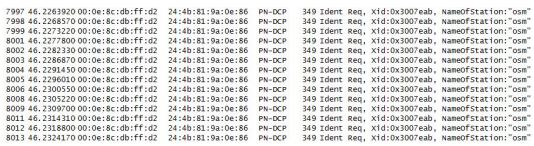

Fig. 10. PROFINET/DCP Protocol Simulation packet list

시뮬레이션 결과 평균 전송 간격은 4μs로 나타났다. 전송과정에서의 스니핑 공격을 수행할 경우 다음 Fig.12.와 같이 패킷에 포함된 데이터를 전부 확인하는 것이 가능하다.

공격자가 스니핑 공격을 수행할 경우 PFOFINET/DCP 프로토콜의 패킷이 지닌 내용을 별다른 조치를 취하지 않고 식별할 수 있다. 이러한 문제점을 극복하기 위해 제안한 프로토콜인 PROFINET/DCP 프로토콜은 Triple-DES를 통해 Data Block 필드에 적재된 데이터를 암호화하고 Data Block 필드의 뒷부분에 적재하여 전송하

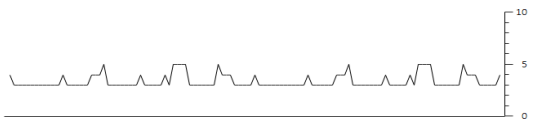

Fig. 11. PROFINET/DCP Protocol transmition interval

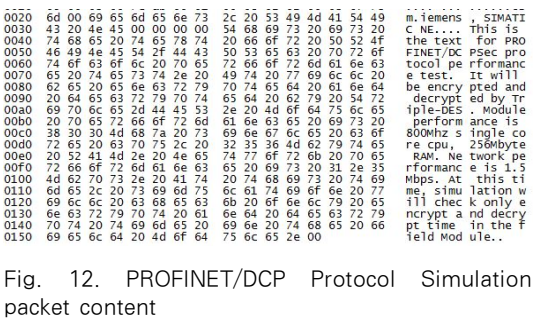

Fig. 12. PROFINET/DCP Protocol Simulation packet content

게 된다. 이때 Triple-DES의 키는 앞서 성능을 예상하기 위해 사용한 것과 동일한 112bit의 길이를 가지며 암호화 및 복호화 키는 사전에 분배, 보호되고 있다는 것으로 가정한다. 암호화는 Application 계층에서 이루어지고 데이터 전송 시간은 전송 발생 시 측정한다.

Fig.13.과 Fig.14.와 같이 데이터 전송 간격은 8μs~13μs이며 평균 전송 간격이 10μs로 전송 간격이 다소 늘어난 것을 알 수 있다. 이러한 전송 간격 증가는 암호화 과정에서 발생하는 것으로 국제 표준에서 요구하는 4ms 의 전송 허용 시간에 비하여 매우 작은 수치이므로 DCPSec의 실제 적용 시에도 큰 영향을 미치지 않는다. MITM 공격 중 스니핑 공격에 대한 방어 효과는 다음 Fig.15.와 같다.

패킷의 Authentication Data Block은 암호화되어 공격자가 알 수 없는 형태로 보이며 인증은 암호화된 데이터를 복호화하여 평문을 생성하고, 이를 사용자 데이터와 비교하여 수행한다. 또한 공격자는 암호화 및 복호화에 사용된 키를 습득할 수 없으므로 네트워크 통신의 중간에서 패킷을 변조, 위조하는 형태의 MITM 공격을 수행할 수 없다. 공격자가 임의의 키를 통해 DCPSec 패킷을 생성, 전송한다 하여도 인증과정을 통해 방어할 수 있어 이러한 암호화 및 인증은 프로토콜이 MITM 공격에 상당한 내성을 가질 수 있게 한다.

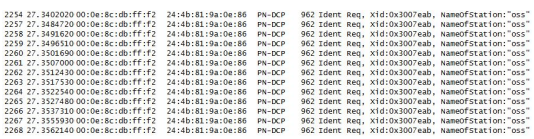

Fig. 13. PROFINET/DCPSec Protocol Simulation packet list

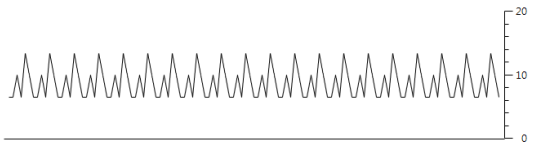

Fig. 14. PROFINET/DCPSec Protocol transmition interval

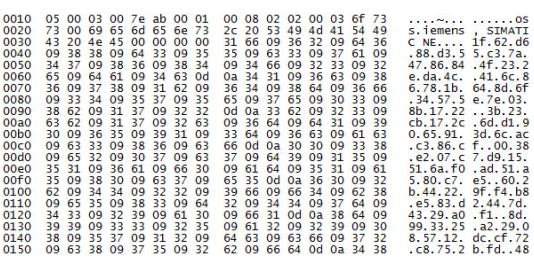

Fig. 15. PROFINET/DCPSec Protocol Simulation packet content

따라서 인증 데이터 필드를 추가하여 개선한 DCPSec은 산업제어시스템에서 안정적으로 동작할 수 있을 뿐만 아니라 인증 데이터 필드를 통해 MITM 공격을 효과적으로 방어할 수 있다. DCP 프로토콜과 DCPSec 프로토콜의 시뮬레이션 및 결과 비교는 다음 Table 5.와 같다.

Table 5. DCP and DCPSec Simulation Result Comparison

Category	DCP	DCPSec
Authentication Guarantee	X	O
Integrity Guarantee	X	O
Defence MITM Attacks	X	O
Transmission Interval	3μs	10μs
Transmission Delay	23μs	34μs
Transmission time Standard Compliance	O	O

VII. 결 론

본 연구에서는 실제 산업제어시스템의 네트워크 트래픽 데이터를 분석하여 문제점을 식별하고 그 해결방안으로 PROFINET/DCP 프로토콜에 인증 데이터를 추가하여 향후 발생할 수 있는 공격을 방어하기 위한 개선 방안을 제시하며 개선된 프로토콜이 산업제어시스템의 응답시간에 미칠 수 있는 영향을 분석하였다. A 발전소의 산업제어시스템 환경에서 이용하는 PROFINET/DCP 네트워크 트래픽 데이터를 분석한 결과 기존의 프로토콜은 인증과정이 부재하여 많은 위협을 안고 있다. 따라서 본 연구는 DCP 프로토콜이 갖는 문제점을 보완하기위해 DCPSec을 제안하였으며 이는 패킷 무결성을 보장하고 패킷 변조 공격, 패킷 스니핑, 패킷 위조 공격을 방어할 수 있다. 개선된 프로토콜은 향후 제어시스템 침해를 방지하고 선제 예방조치로 작용하여 시스템 보안능력을 강화할 수 있다. 본 연구에서 분석한 PROFINET/DCP 패킷은 실제 산업제어현장의 트래픽으로 제안한 프로토콜이 현실적인 대안이 될

수 있으며 산업제어시스템의 보안 취약점을 해결하는 데 큰 역할을 수행할 수 있을 것으로 예상된다.

References

[1] SCADA, http://en.wikipedia.org/wiki/SCADA

[2] STUXNET, http://en.wikipedia.org/wiki/Stuxnet

[3] Mai Kiuchi, Eiji Ohba and Yoshizumi Serizawa, "Customizing Control System Intrusion Detection at the Application Layer," The SCADA Security Science Symposium, pp. 2-11, Jan. 2009

[4] Hadeli, Ragnar Schierholz, Markus Braendle, Cristian Tuduce and Sebastian Obermeier, "Leveraging Determinism in Industrial Control Systems for Advanced Anomaly Detection and Reliable Security Configuration," The SCADA Security Science Symposium, pp. 1-8, Sept. 2009

[5] Ron Gula, "Identifying Attacks on Control Systems by Scripting Event Aggregation and Correlation," The SCADA Security Science Symposium, pp. 1-6, Oct. 2006

[6] Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner and Alfonso Valdes, "Using Model-based Intrusion Detection for SCADA Networks," Proceedings of the SCADA security scientific symposium, pp. 1-12, Jan. 2007

[7] Wanjib Kim, Huykang Kim, Kyungho Lee and Heungyoul Youm, "Risk Analysis and Monitoring Model of Urban SCADA Network Infrastructure," Journal of The Korea Institute of Information Security & Cryptology, 21(6), pp. 67-81, Jun. 2011

[8] http://en.wikipedia.org/wiki/PROFINET

[9] PROFINET Manual, http://www.profinet.felser.ch/index.html?dcp_frame.htm

[10] Form of PROFINET DCP packet, http://www.industrialnetworx.com/forum/profinet/com-flag-not-set

[11] PROFINET protocol family, http://wiki.wireshark.org/PROFINET

[12] PROFINET Overview - DCP addressing and subnetting, http://us.profibus.com/docs/pi_white_paper_profinet_it_en_v1_0.pdf

[13] PROFINET Addressing, PROFINET System Description Technology and Application, http://www.automation.com/pdf_articles/profinet/PI_PROFINET_System_Description_EN_web.pdf

[14] DHCP Addressing, http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=29451913&nodeid0=18977720&load=treecontent&lang=en&siteid=cseus&aktprim=0&objaction=csview&extranet=standard&viewreg=WW

[15] Constructing and sending DHCP messages, http://www.freesoft.org/CIE/RFC/2131/20.htm

[16] Pauline Koh, Hwajae Choi, Seryoung Kim, Hyukmin Kwon and Huykang Kim, "Intrusion Detection Methodology for SCADA system environment based on traffic self-similarity property," Journal of The Korea Institute of Information Security & Cryptology, 22(2), pp. 267-281, Apr. 2012

[17] Munir Majdalawieh, Francesco Parisi-Presicce and Duminda Wijesekera, "DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework," Advances in Computer, Information, and Systems Sciences, and Engineering, 2006 Springer, pp. 227-234, Oct. 2006

[18] Kim and Montgomery, "Behavioral and Performance Characteristics of IPSec/IKE in Large-Scale VPNs," Proceedings of the IASTED International Conference on Communication Network and Information Security, pp. 10-12, Dec. 2003

[19] Gordon Clarke and Deon Reynders,

"Practical Modern SCADA Protocols:DNP3, 60870.5 and related systems," pp. 10-15, Newnes. 2004
〔20〕 Erich Nahum, Sean O'Malley, Hilarie Orman, and Richard Schroeppe, "Towards High Performance Cryptographic Software," Citeseer, pp. 1-5, Oct. 1995
〔21〕 Bruce Schneier, Kelsey, J., Whiting, D., Wagner, D., Hall and C. and Ferguson N., "Performance Comparison of the AES Submissions," NIST, pp. 1-20, Feb. 1999
〔22〕 IEC 61850, http://en.wikipedia.org/wiki/IEC_ 61850
〔23〕 Sangkyo Oh, Hyunji Chung, Sangjin Lee and Kyungho Lee, "Advanced Protocol to Prevent Man-in-the-middle Attack in SCADA System," International Journal of Security and Its Applications, vol. 8, no. 2, pp. 1-8, Jan. 2014
〔24〕 BAGARIA, Sankalp PRABHAKAR, Shashi Bhushan and SAQUIB Zia, "Flexi-DNP3: Flexible distributed network protocol version 3 (DNP3) for SCADA security. In: Recent Trends in Information Systems (ReTIS)," 2011 International Conference on. IEEE, pp. 293-296, Dec. 2011
〔25〕 MAJDALAWIEH, Munir WIJESEKERA and Duminda, "DNPSec Simulation Study." In Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, 2007 Springer, pp. 337-342, Jan. 2007

〈저자소개〉

고 무 성 (Ko Moo Seong) 학생회원
2014년 2월: 한국산업기술대학교 컴퓨터공학과 학사
2014년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 제어시스템, 위험관리, 개인정보보호정책

오 상 교 (Oh Sang Kyo) 학생회원
2013년 2월: 광운대학교 컴퓨터소프트웨어전공 학사
2015년 2월: 고려대학교 정보보호대학원 석사
〈관심분야〉 정보보호컨설팅, 위험관리, 개인정보보호정책

이 경 호 (Kyung Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월~현재: 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 위험관리. 정보보호컨설팅. 정보보호 및 개인정보보호정책