정 보 보 호 학 회 지
제24권 제5호, 2014. 10

배전DAS-업무망 보안 이슈 및 물리적 일방향 자료전달 시스템 적용 방안

김 지 희*, 김 진 철**, 박 성 완***, 송 주 영****

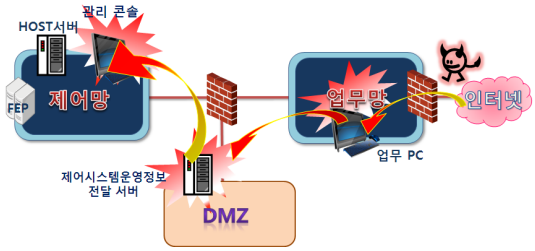
요 약

제어시스템은 일반 업무환경에서 사용하고 있는 시스템과는 달리 업무망과 분리되어 운영되며, 비공개 제어프로토콜 사용으로 해커나 악성코드에 의해 사이버공격을 받을 가능성이 없다고 인식되어 왔다. 그러나 2010년 스턱스넷(Stuxnet) 악성코드가 이란의 핵시설 제어시스템에 침투하였고 2012년 듀크, 플레임 등 제어시스템을 대상으로 한 위협이 증가하게 되면서 제어시스템과 업무망 연계 지점의 보안 위협을 제거하기 위한 방안으로 물리적 일방향 자료전달 시스템의 도입이 추진되어 왔다. 본 논문에서는 배전DAS 업무망 연계를 위한 물리적 일방향 자료전달 시스템 구현에 대해서 설명하고 실증에 따른 결과를 제시한다.

Ⅰ. 서 론

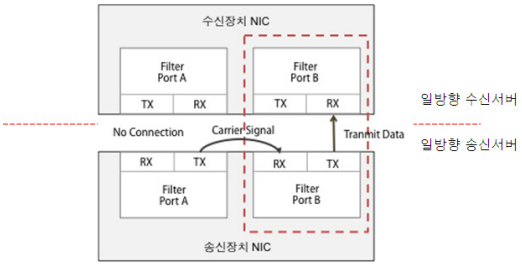
현재 스마트그리드 지향으로 전력망에 ICT기술을 적용하여 양방향으로 전력정보를 교환하는 전력망을 운영하고 있다. ICT기술의 적용은 전력망의 양방향 정보교환이라는 편의성을 제공한다. 반면, ICT기술은 보안 취약성을 그대로 가지고 있다. 그림 1은 인터넷을 통한 업무망의 악성소프트웨어의 감염 경로를 보여주고 있다. 기반시설 제어망과 업무망은 네트워크로 연결되어 감시관리하고 업무망에는 인터넷망이 연결되어 전 세계적으로 연결되어 정보를 교환한다. 네트워크망으로 연결되어 있기 때문에 스팸메일, 악성 웹페이지 접속으로 업무PC는 악성 소프트웨어(바이러스, 스파이웨어, 멀웨어)로 쉽게 감염된다. 감염된 업무PC의 악성 소프트웨어는 침입차단시스템 설정 오류, 서버 취약점을 통하여 제어시스템 운영 서버를 2차 감염시키고 제어망을 통하여 침입차단 시스템 설정 오류, 클라이언트 취약점을 공격하여 제어 서버를 감염 시킨다. 이렇게 전력 제어시스템까지 악성코드에 감염이 된다면 전력기반 시설의 마비, 파괴, 악의적인 전력제어 등으로 전력기반 시설이 붕괴될 수 있다. 이로 인한 전력산업 파급 효과와 국가 경제적으로 큰 손실을 초래한다.

국가정보원에서는 국가기반시설 전자제어시스템 보안가이드라인을 작성하여 기반시설 공공기관들로 하여금 안전한 제어망 보안대책을 제시하였다. 이 보안가이드라인에서 안전한 제어망 연동기법으로 물리적 연결선 차단을 통한 일방향 네트워크 연결을 소개하였다. 한전은 외부로부터의 해킹 및 보안 사고에 의한 중요자료 유출을 방지하기 위해 네트워크 간 자료전송 기술 중 하나인 물리적 일방향 자료전달 장치[1]의 도입을 추진하고 있다. 물리적 일방향 자료전달 시스템은 우선 배전DAS망-업무망에 연계 부분에 구축하고 업무망에서 제어망으로의 데이터 회선을 그림 2와 같이 제거하여 업

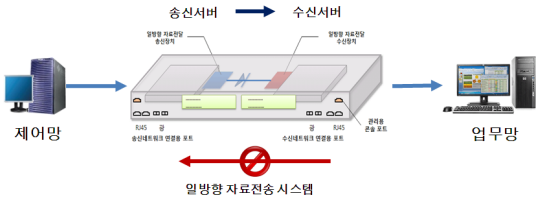


〔그림 1〕 제어망과 업무망 간 보안위험

* 한전KDN 전력IT연구원 기반시설보안연구팀 (k.jihee@kdn.com)
** 한전KDN 전력IT연구원 기반시설보안연구팀 (kjc@kdn.com)
*** 한전KDN 전력IT연구원 기반시설보안연구팀 (adonis@kdn.com)
**** 한전KDN 계통사업처 계통제어팀 (sjy7395@kdn.com)



〔그림 2〕 물리적 일방향 광 케이블 개념도



〔그림 3〕 제어시스템에 적용된 일방향 자료전달 시스템

무망에서의 침입가능성을 완전히 차단한다. 이는 제어망의 단말장치나 센서를 통한 계측 정보와 시스템 운영을 위한 감시 정보는 업무망으로 전달되어 업무효율을 유지하나 업무망에서 제어망으로의 원천적인 차단으로 제어망의 보안을 유지할 수 있게 해준다. 일방향 자료전달 시스템은 그림 3과 같이 네트워크상에서 제어망과 업무망의 연계 부분에 위치한다. 물리적으로 제어망에서 업무망을 연결하나 반대로는 연결되지 않는다는 것이 중요한 보안 요소이다.

Ⅱ. 배전DAS 업무망 연계를 위한 물리적 일방향 자료전달 시스템 구현 시 고려대상

안전과 유지가 최우선인 제어시스템인 배전DAS망에서 기존의 서비스를 변경하는 것은 쉽지 않다. 따라서 기존의 서비스를 최대한 변경하지 않고 적용할 수 있도록 일방향 자료전달 시스템을 구현하였다. 배전DAS망의 경우 고려할 점으로는 다음과 같다.

· N:N의 서버-클라이언트 형태
· 전송 데이터 신뢰도

2.1. N:N의 서버-클라이언트 일방향 통신

배전DAS망은 본사 수집서버 3대와 전국 41개의 센터(클라이언트)로 구성되어 3:41의 통신을 하는 형태이다. 일반적인 서버-클라이언트 구조는 1:N의 형태이므로 기존의 일방향 자료전달 시스템[2,3]은 이를 지원하지 못하고 하나의 포트에 하나의 클라이언트의 연결만을 지원한다. 일방향 자료전달 시스템에 대한 안정성 측면에서는 좋은 선택일 수 있지만 기존의 제어시스템의 형태를 바꿔야한다는 문제가 있다.

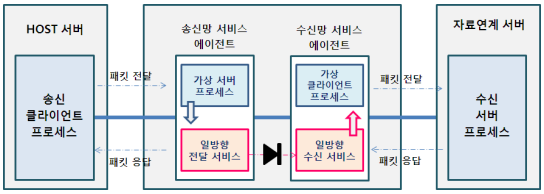
2.2. 전송 데이터 신뢰도

센터에서 본사 수집서버로 전송되는 데이터는 고장정보, 배전망상태, 최대부하 등 수집서버에서 가공하여 실제로 사용하는 중요 정보이다. 기존 일방향 자료전달 시스템의 경우 TCP/IP와 같은 양방향 프로토콜을 UDP와 같은 단방향 프로토콜로 변경하면서 일방향 자료전달 시스템을 구현한 대신 TCP/IP통신에서의 신뢰성을 100% 확보하는 데는 어려움이 있다.

Ⅲ. 배전DAS 업무망 연계를 위한 물리적 일방향 자료전달 시스템 구현 및 실증

일방향 자료전달 시스템은 하나의 외함에 송, 수신서버로 구성되어 있다. 송신서버는 제어망의 송신 클라이언트와의 통신을 담당하고 일방향 구간으로 데이터 전송을 담당하는 송신망 에이전트, 일방향 자료전달 송신서버의 프로세스를 관리하는 관리인터페이스, 그리고 네트워크 디바이스 드라이버와 같은 네트워크 인터페이스로 구성되어 있다. 수신서버는 기본적으로 송신서버와 동일하나 전달된 데이터를 처리하는 수신망 에이전트 부분이 상이하며 수신망 에이전트에서 로그 및 데이터 관리를 하며 프로세스를 관리하는 관리인터페이스, 네트워크 인터페이스로 구성되어 있다. 송, 수신서버간에는 그림 2에서 살펴본 바와 같이 하나의 광케이블로 구성되어있다.

그림 4와 같이 송, 수신서버에 설치되어 있는 서비스 에이전트를 통해 제어망 내 송신 시스템에서 전달된 데이터를 일방향 자료전달 시스템을 통해 수신망 서비스 에이전트로 전송하며, 수신망 서비스 에이전트는 일방향 시스템을 통해 수신된 데이터를 업무망 내 수신 시스템으로 전송한다.



〔그림 4〕 일방향 자료전달 시스템 구성도

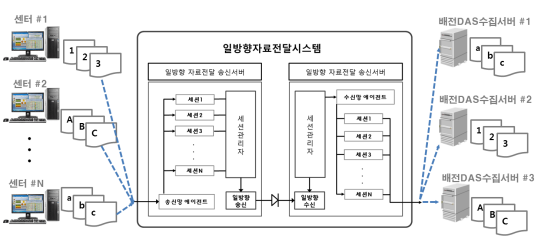
3.1. N:N의 서버-클라이언트 일방향 자료전송

일반적인 네트워크는 서버-클라이언트 관계가 1:N으로 구성되어 있다. 하지만 기존의 일방향 자료전달 시스템은 1:1 서비스의 형태를 취하고 있다. 서버 역할을 하는 서비스를 구동하고 있으면 수신 대기 중인 Port 하나당 하나의 클라이언트만 접속이 가능하다. 이는 일방적인 네트워크의 서버-클라이언트 구조와도 상이하고 동일 서비스라도 클라이언트의 수만큼 Port를 할당해야 한다[4].

이를 해결하고 제어시스템의 서버-클라이언트 구조를 지원하기 위해서 N:N 멀티세션 방식을 사용하였다.

그림 5 N:N 서버-클라이언트에서의 멀티세션 지원 구조에서 송신서버의 송신망 에이전트와 수신서버의 수신망 에이전트는 각각 업무망의 서버 역할과 제어망의 클라이언트 역할을 수행한다. 제어망의 클라이언트는 송신망 에이전트로 접속해 기존의 업무망 서버로 자료를 전송하던 것처럼 동일하게 동작하도록 지원하며 세션관리자는 세션 정보 및 클라이언트의 네트워크 정보를 획득하여 세션을 관리하기 위한 정보로 가공한다. 이 정보를 일방향 구간(광 케이블)을 통해 송신할 때 추가하여 수신서버로 전송한다.

수신서버는 송신서버로부터 수신된 세션정보를 분석하여 수신망 에이전트로 전달한다. 수신망의 세션 관리자는 세션 정보를 이용하여 업무망의 서버와 동일한 세션을 생성, 관리한다. 그리고 제어망 클라이언트로부터



〔그림 5〕 N:N 서버-클라이언트에서의 멀티세션 지원 구조

전송된 데이터에 해당되는 세션을 통하여 전송한다.

이 구조와 절차를 통해 멀티세션을 지원하게 되며 클라이언트와 서버는 기존의 통신방식으로 데이터를 전달함으로 별도로 시스템을 수정할 필요가 없다.

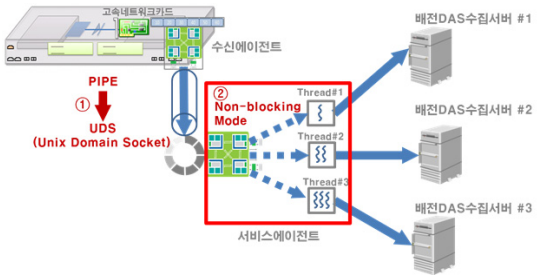
3.2. 전송 데이터 신뢰도 향상

TCP프로토콜과 UDP프로토콜의 가장 큰 차이는 데이터 신뢰도이다. 연결지향적인 TCP프로토콜을 사용하여 데이터를 전송하는 경우 데이터 전송 전 연결상태를 확인하고 데이터 전송 중에도 빠진 패킷에 대해 재전송을 요구하므로 전송신뢰도가 100%이다. 그에 반해 UDP프로토콜을 사용하여 데이터를 전송하는 경우 비연결형으로 신뢰성을 보장하지 않는다. 기존 TCP프로토콜 기반의 통신방식을 제공하는 배전DAS망에 물리적 일방향 자료전달 시스템을 도입함으로써 일방향 구간에 대해서는 UDP프로토콜을 사용하여 자료를 전송하는 방식을 채택하였다.

배전DAS 제어망에서 업무망으로 전송하는 데이터의 경우 중요 정보를 포함하고 있으며 실업무에 사용되는 데이터이므로 데이터의 신뢰도를 향상시키는 것이 매우 중요하다. 이에 실제 일방향 통신이 이루어지는 송신서버와 수신서버간의 일방향 구간으로 데이터를 전달 시, Sequence Number 필드를 추가하여 수집서버에서 받은 데이터를 재가공할 때 패킷의 누락 여부를 알 수 있게 하였다.

또한 일반적인 네트워크 통신의 경우 출발지와 목적지가 대부분 정해져있어 데이터흐름과 크기를 가늠할 수 있다. 하지만 배전DAS망은 전국 41개의 센터에서 데이터가 동시에 전송될 수도 있고 실시간 데이터의 경우 간헐적으로 전송되기 때문에 흐름과 크기를 가늠할 수 없다는 점도 고려하여야 했다.

기존 파이프방식의 IPC통신으로 일주일간의 테스트를 거치는 동안 데이터 용량을 초과하여 블록상태가 되는 경우가 발생하였다. 이에 수신에이전트에서 각 서비스 에이전트로 데이터를 전송하는 Blocking Mode에서 멈춤 현상이 발견 되어 오류가 발생 한 서비스에이전트뿐 아니라 전체 서비스에이전트를 멈추게 만들었다[5]. 그림 6과 같이 기존의 PIPE 방식을 UDS로 변경하여 기존의 문제점을 해결하고 Blocking-Mode를 Non-Blocking Mode로 변경하여 block되어 다른 서비스 에



〔그림 6〕 데이터 신뢰도를 위해 기존 시스템에서의 수정

이전트나 시스템을 영향을 미치지 않도록 변경하였다.

Ⅳ. 실증 결과

2013년 10월~2014년 현재까지 배전DAS망의 일방향 시스템 적용을 실증하였으며 초기에 발생되는 문제점을 해결하여 본실증은 2014년 4월 22일부터 진행되었다.

그림 7은 실증기간 동안 패킷로스 혹은 시스템오류를 검출하기 위해 통신구간을 나눠 확인한 것이다. 송신 클라이언트로부터 전송되는 데이터가 최종 수집서버에 도달하는 데 있어 연계 구간을 4군데로 보았다. ① 송신 클라이언트와 일방향 시스템 송신서버의 연계접점 ② 일방향 송신서버 ③ 일방향 수신서버 ④ 일방향 수신서버와 DAS수집서버의 연계접점. 각 구간의 로그를 분석

〔그림 7〕 배전DAS 업무망 연계에 있어서의 통신구간

〔표 1〕 배전DAS 업무망 연계에 있어서 각 구간 별 데이터 전송속도 및 손실율

	①	②	③	④
통신구간	DAS 클라이언트 → 일방향 송신서버	일방향 송신서버 → 일방향 수신서버		일방향 수신서버 → DAS수집 서버
데이터 처리속도	400~800 Mbps	1Gbps		400~800 Mbps
데이터 손실율	0%	0%		0%

하여 받은 데이터 및 패킷 사이즈, 보낸 데이터 및 패킷 사이즈 그리고 받고 보낸 시간을 계산하여 데이터 처리 속도 등을 계산하였다. 33일간의 실증기간 동안 일방향 시스템에서의 메모리 누수나 데이터손실은 발견되지 않았으며 데이터 용량에 따른 시스템 부하도 발견되지 않았다.

Ⅴ. 결론 및 향후 연구

물리적 일방향 자료전달 시스템의 원리는 단순하지만 이를 실제 전력제어시스템에 적용하기까지 많은 부분을 해결해야했다. 우선 비정상적인 통신 종료에 대한 부분을 예외처리하고 프로세스가 다운되지 않도록하는 안정화 작업이 선제되어야했다. 일방향 자료전달 시스템 운영에 있어 효율성을 위해 멀티세션으로 통신할 지 안정성을 위해 포트로 통신할 지를 결정하고 그에 맞게 송·수신 에이전트를 최적화하였다. 최적화 후 데이터 전송 신뢰성과 시스템 안정성을 높일 수 있는 방안을 추가로 구현하였다. 배전DAS망의 경우 N:N의 서버-클라이언트 구성에 따른 멀티세션 통신과 일방향으로 전송되는 데이터의 신뢰도 및 시스템 안정성을 향상시키기 위한 내부 IPC통신을 UDS방식으로 변경하여 구현하였다.

향후 전력망 이외의 다른 제어망 적용시 효율적으로 운영이 가능하도록 데이터베이스를 이용한 자료전달 서비스 에이전트 개발에 대한 연구와 네트워크 부하에 대비한 절체방안인 이중화 설계에 대한 연구가 진행 중에 있다.

참 고 문 헌

[1] Pascal Sitbon, Arnaud Tarrago, Pierre Nguyen, “Enabling Secure Information Exchange from a Less Secure Zone to a Control System Zone in a Critical Infrastructure”, *Proceedings of the SCADA Security Scientific Symposium,* Digital Bond Press, p.10, 2003.

[2] WF-SME. [Online]. Available : http://waterfall-security.com

[3] Data diode. [Online] Available : http://owlcti.com

[4] 김경호, 장엽, 김희민, 윤정한, 김우년, “제어망 특성을 반영한 물리적 일방향 자료전달 시스템 설계”, *정보과학회논문지 : 정보통신*, pp126-130, 2013.

〈저 자 소 개〉

김 지 희 (KIM Jihee)
비회원

2011년 8월 : 금오공과대학교 전자공학부 졸업
2011년 8월~현재 : 한전KDN 전력IT연구원 근무
관심분야 : 전자공학, 통신공학, 정보보호

박 성 완 (PARK Sungwan)
비회원

2001년 2월 : 연세대학교 대학원 석사 졸업
2001년 3월~현재 : 한전KDN 전력IT연구원 근무
관심분야 : 소프트웨어공학, 정보보안, 정보통신

김 진 철 (KIM Jincheol)
정회원

2006년 8월 : 광운대학교 대학원 박사 졸업
1996년 12월~현재 : 한전KDN 전력IT연구원 근무
관심분야 : 암호알고리즘, 정보보안

송 주 영 (Song Jooyoung)
비회원

2010년 8월 : 방송통신대학교 미디어영상학과 졸업
1997년 11월~현재 : 한전KDN 계통제어팀 근무
관심분야 : 네트워크, 기반시설보안, 전자공학