https://doi.org/10.5392/JKCA.2018.18.08.102

빌딩시설 제어시스템용 안전한 망간 자료전송 방안

Secure Data Transmission Scheme between Network for Building Facilities Control System

조인준
배재대학교 사이버보안학과

In-June Jo(injune@pcu.ac.kr)

요약

비 보안영역의 외부인터넷과 보안영역의 내부업무망간에 적용된 기존의 망간 자료전송기술을 빌딩시설관리 SCADA시스템 제어망에 그대로 적용할 경우에 다양한 문제들이 도출된다. 기존의 망간 자료전송기술은 모든 데이터를 대상으로 블랙리스트 기반의 보안기법이 적용되기 때문에 고 복잡성 및 고 비용이 수반된다. 하지만, 빌딩시설관리 SCADA제어시스템에서 유통되는 데이터의 특성은 소수의 정형적인 제어 데이터가 반복성과 주기성을 갖기 때문에 이를 대상으로 화이트리스트 기반의 보안기법 적용이 가능하다. 이를 통해서 망간 자료전송에 적용된 보안기술이 단순화되어 저 비용으로 빌딩시설관리 SCADA시스템 제어망 구축이 가능하다. 본 논문에서는 이러한 문제점들을 정리하고 이를 해결하는 방안을 제시하여 빌딩시설관리 SCADA제어시스템에 특화된 빌딩 제어망 구축방안을 제안하였다.

■ 중심어 : | 망간자료전송기술 | 빌딩시설관리 제어망 | SCADA시스템 | 망 분리 |

Abstract

The existing data transmission technology applied between the non-secure external internet and the secure internal business network has various problems when applied to the building facility management SCADA system control network. Traditional inter-network data transfer technologies involve high complexity and high costs because blacklist-based security techniques are applied to all data. However, whitelist-based security techniques can be applied to data distributed in Building Facility Management SCADA control systems because a small number of structured control data are repeatable and periodic. This simplifies the security technology applied to inter-network data transmission, enabling building facility management SCADA system control network deployment at low cost. In this paper, we proposed building control networks specialized in building facility management SCADA control systems by providing solutions to address and address these problems.

■ keyword : | Building Control | SCADA | Control Network | Network Separation | Security |

* 본 논문은 2018학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임
접수일자 : 2018년 07월 09일
심사완료일 : 2018년 08월 17일
수정일자 : 2018년 08월 17일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

외부데이터가 인터넷을 통해서 실시간으로 반영되어(예, 기상정보, 재난정보 등) 운영되는 빌딩시설관리 SCADA(Supervisory Control And Data Acquisition) 제어시스템은 최고의 보안성과 가용성이 보장되어야한다. 여기에서 최고의 보안성은 해커가 인터넷을 통해서 빌딩시설관리 SCADA제어시스템을 직접 해킹공격을 할 수 없도록 보안체제를 갖추어야 한다는 것이다. 그리고 최고의 가용성은 앞에서 전제한 최고의 보안성 보장이란 전제하에서 어떤 상황에서든 365일 24시간 외부데이터를 빌딩시설관리 SCADA제어시스템에 반영할 수 있는 환경을 갖추어야 한다는 것이다.

이에 대한 보안대책으로 정부는 사이버해킹에 안전한 행정업무 처리 및 SCADA제어시스템 운영관리를 위해 외부 인터넷과 독립적으로 내부 업무망과 SCADA시스템 제어망을 각각 분리운영을 원칙으로 하고 있다[그림 1][1].

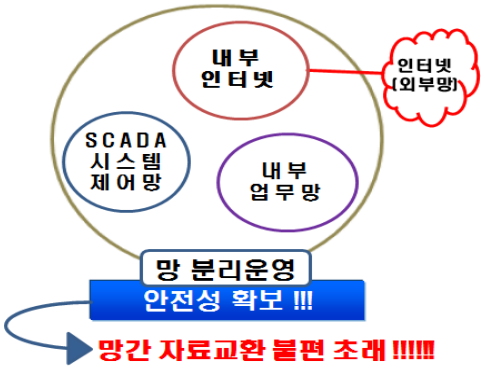

그림 1. 망 분리 개념도

이는 각각의 망 분리를 통해서 외부인터넷으로부터 침입하는 수많은 다양한 해커들을 원천적으로 차단하여 내부 업무망과 SCADA시스템 제어망의 안전성 확보를 최대의 정책적 목표로 한 것으로 판단된다[4][5]. 하지만, 이를 준용하여 망을 분리하여 운영하면 망간의 자료전송이 필요할 경우 USB(Universal Serial Bus)와 같은 수작업에 의한 반입 및 반출만을 허용하기 때문에 여러 불편을 초래했다[1].

이러한 불편해소를 위해『IT보안인증사무국』에서는『망간 자료전송제품 보안요구사항 V1.0』을 제정하였다. 즉, 비 보안영역의 외부인터넷과 보안영역의 내부 업무망간의 자료전송 시 이를 만족시켜 자료전송 자동화를 실현하도록 강제하고 있다[2]. 하지만, 현재 이를 준용하여 시판되고 있는 망간 자료전송제품은 블랙리스트기반의 보안기법이 적용된 제품이다. 즉, 내부 업무망과 외부 인터넷 간에 불특정한 모든 응용을 대상으로 범용자료가 망간에 안전하게 반입/반출되도록 보안기술이 설계됨에 따라 매우 복잡하고 고가인 것이 사실이다.

하지만, 빌딩시설 SCADA시스템 제어망은 일반적인 내부 업무망과 다른 형태의 응용과 자료가 유통되는 특성을 진니다. 즉, 빌딩 SCADA시스템 제어망은 특정의 응용과 이에 특화된 단순하고 반복적이고 주기성을 지닌 자료의 반입 및 반출이 특정 외부인터넷과 이루어진다는 점을 들 수 있다. 이러한 특성 때문에 현재 시판되고 있는 블랙리스트기반의 보안기법을 사용한 망간자료전송제품을 그대로 활용하기에는 복잡성 및 고 비용 측면에서 부적합한 것으로 판단된다.

다음으로 주목할 것은 외부데이터가 인터넷을 통해서 실시간으로 반영되어 운영되는 빌딩시설관리 SCADA 제어시스템이 고 가용성이어야 한다는 점이다. 현재의 환경에서 가용성을 저해하는 주요원인을 살펴보면, 빌딩에 설치된 공용인터넷의 고장 및 해킹 의한 외부데이터 전송방해를 들 수 있다. 그리고 인터넷이 설치되어 있지 않은 빌딩들에 대해서는 가용성을 보장할 수 없다는 문제점을 지닌다.

결론적으로 본 논문에서는 이러한 보안성 및 가용성에 대한 현안 문제점들을 해결하기 위해, 빌딩시설관리 SCADA시스템만의 특성을 반영한 망간자료전송 방안을 제안하였다.

II. 연구배경

현재 빌딩시설관리 SCADA시스템 제어망은 3가지로 운영된다. 첫째는 다른 망과 완전 폐쇄망으로 운영되는 경우, 둘째는 외부 인터넷에 직접 연결되어 운영되는 경우, 마지막으로는 외부 인터넷과 망 분리가 되고 범

용적인 망간 자료전송 보안요구사항을 만족하는 제품이 설치되어 운영되는 경우로 나눌 수 있다[그림 2][1][2].

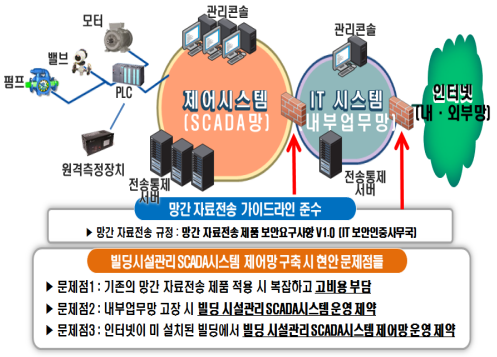

그림 2. 현재 망 분리 및 망간 자료전송 개념도

첫 번째 형태로 운영될 경우는 외부해커들로 부터 빌딩시설관리 SCADA시스템 제어망이 고립되기 때문에 가장 보안에 안전하나 외부인터넷 사이트로부터 제어정보를 실시간으로 제어시스템에 반영할 경우는 지원이 불가한 치명적인 문제를 지닌다. 두 번째 형태로 운영될 경우는 외부 인터넷 해커가 직접적으로 빌딩제어시스템에 침투가 가능하여 가장 보안에 취약한 운영 방법이다. 마지막으로 [그림 2]와 같이 운영되는 경우는 『IT보안인증사무국』에서 요구하는 망간자료전송 보안요구사항을 만족하나 빌딩시설관리 SCADA시스템의 특성이 반영되지 않아 구축비용이 고가라는 점, 그리고 내부업무망 혹은 외부 인터넷 고장 시 가용성에 제약을 받게 되고, 마지막으로 인터넷이 미설치된 빌딩들에 대해서는 가용성을 보장 할 수 없게 된다.

상기에서 살펴 본 현안 문제점들이 시사하는 바는 빌딩시설관리 SCADA제어시스템에 특화되고 효율적인 망간 연동 및 자료전송방안이 현재로서는 부재하다는 점을 들 수 있다. 이러한 문제들에 대한 해결책 제안이 본 논문의 연구배경이다. 즉, 본 논문에서는 상기에 언급된 문제점들을 제거하여 빌딩시설관리 SCADA제어시스템에 특화된 새로운 망간 연동 및 자료전송 방안을 제안한 것이다.

Ⅲ. 안전한 빌딩시설관리 SCADA제어망 연동 및 자료전송 방안

3.1 빌딩시설관리 SCADA제어시스템 특성 요약

빌딩시설관리 SCADA시스템 제어망은 일반업무망과 다른 특성을 지닌다. 첫째, 외부 인터넷 사이트로부터 실시간으로 전송되는 데이터가 극히 제한적인 특정 사이트로부터 극히 제한적인 제어데이터가 유입되어 제어시스템에 반영된다는 점을 들 수 있다. 둘째, 빌딩시설관리 SCADA시스템 제어망은 외부인터넷이 구축되어 있지 않은 건물에서도 운영될 수 있다. 이러한 환경에서는 외부 인터넷사이트로부터 실시간으로 제어데이터를 반영하여 운영되는 빌딩제어시스템은 운영이 불가능할 수 있다. 이를 극복하는 방법으로 외부인터넷 제어 데이터를 예측하는 방법을 들 수 있으나 이는 매우 복잡하고 예측된 데이터의 정확성 확보가 관건이 되는 제약을 지닌다. 셋째, 빌딩시설관리 SCADA제어시스템의 가용성은 100%에 근접하도록 유지되어야 한다. 빌딩제어망이 외부인터넷으로부터 연동되는 경우 인터넷 고장 시 빌딩제어시스템 운영에 제약을 주어 가용성을 떨어뜨리는 결과를 가져온다.

상기와 같은 빌딩시설관리 제어시스템만의 특성이 반영된 망 연동 및 자료전송 보안요구사항을 만족하는 방안을 다음절에 제안하였다.

3.2 안전한 빌딩시설관리 SCADA시스템 제어망 구성방안

II장의 연구배경에서 현재 빌딩시설관리 SCADA시스템 제어망의 현안 문제점을 정리하였고, 3.1절에서 빌딩시설관리 SCADA제어시스템의 특성을 요약하였다. 여기에서 제시된 문제점들을 제거하고, 더불어 제시된 빌딩시설관리 SCADA시스템만의 특성을 반영하여 본 논문에서 제안하는 빌딩시설관리 SCADA시스템 제어망의 전체적인 구성방안은 [그림 3]과 같다.

[그림 3]에서 보듯이 가장 큰 특징은 기관 내 비 보안영역으로 정의되는 빌딩시설관리 SCADA시스템 전용 외부망을 기존의 외부 인터넷 라우터를 사용하지 않고

독립적인 이동통신 LTE(Long Term Evolution)모뎀과 초소형 마이크로컴퓨터(예, 라즈베리파이, 오드리드, 오렌지파이 등)를 기반으로 구성함으로써 저 비용으로 구현했다는 점을 들수 있다. 이렇게 구성함으로써 얻을 수 있는 이점을 정리하면 다음과 같다.

첫째, 기관의 내부인터넷의 가용성보다는 이동통신 LTE망의 가용성이 높다는 점이다. 즉, 내부 인터넷의 고장과 관계없이 LTE모뎀을 통해서 외부사이트 제어데이터를 실시간으로 수신하기 때문에 빌딩시설관리 SCADA시스템의 가용성을 제고한 결과를 가져온다. 둘째, 인터넷이 설치되어 있지 않은 빌딩에서도 LTE모뎀을 통해서 빌딩시설관리 SCADA시스템을 손쉽고 편리하게 구축 운영이 가능하다는 점을 들 수 있다. 이는 기관내 모든 빌딩에 공용인터넷을 설치해야 하는 부담을 제거하는 효과도 가져온다.

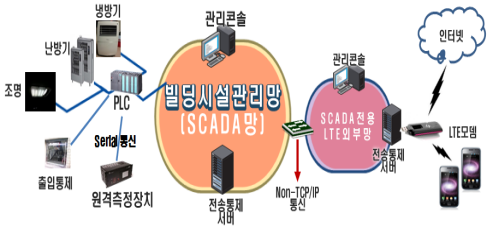

그림 3. 본 논문에서 개발목표인 빌딩시설관리 SCADA 제어시스템 구성도

셋째, 기관 내 내부 업무망과 독립적으로 빌딩시설관리 SCADA시스템 제어망이 운영되기 때문에 빌딩시설관리 제어데이터와 내부 업무망 데이터가 분리되어 제어데이터의 무결성 및 안전성 확보가 용이하다는 점을 들 수 있다. 넷째, 기관 내 빌딩시설관리 SCADA시스템 전용 외부망 구축비용을 현저히 줄일 수 있다. 즉, 빌딩시설관리 제어시스템에 반영되는 제어 데이터는 극히 소수의 정해진 사이트로부터 정해진 소량의 데이터가 생성되어 반영되기 때문에 LTE모뎀과 저가의 초소형 마이크로컴퓨터를 사용하여 간단하게 구축이 가능하다. 다섯째, LTE기반 전용 외부망의 보안성 강화가 용이하다는 점을 들 수 있다. 즉, 빌딩시설관리 제어시스템에 반영되는 제어 데이터가 극히 소수의 정해진 사이트로부터 반복성/주기성/단순성을 특성으로 하여 반입되기 때문에, 해커들의 위험성이 상존하는 불특정 사이트로부터는 접근을 허용하지 않는 화이트리스트 기반의 S/W 방화벽 구현이 용이하고, 방화벽을 통과한 제어데이터에 대해서도 진성데이터만 허용하고 악성데이터를 불허하는 화이트리스트기반의 보안기법을 사용하여 비 보안 영역 내의 LTE 모뎀 기반 SCADA 전용 외부망의 보안성을 저비용으로 손쉽게 강화할 수 있다. 여섯째, 빌딩시설관리 SCADA시스템에 응급상황 발생시 관리담당자 핸드폰에 긴급메시지를 안전하게 전송이 용이하다. 이는 외부로 전송되는 메시지에 대해 보안정책에 따른 전송절차에 따라 LTE모뎀을 활용하기 때문이다.

이상과 같이 비 보안영역에서 빌딩시설관리 SCADA 전용 LTE모뎀기반 전용 외부망을 도입함에 따라 상기에서 정리한 현안 문제점들이 해결되고 빌딩시설관리 제어시스템의 특성이 모두 반영된 것으로 볼 수 있다.

다음 특성은 앞에서 구축한 비 보안영역의 LTE모뎀 기반 빌딩 SCADA시스템 전용 외부망과 보안영역의 빌딩시설관리망 간을 저비용 통신매체로 연동할 수 있다는 점을 들 수 있다. 두 망간에 유통되는 데이터의 특성을 보면, 빌딩시설제어에 특화된 제어데이터가 유입되고 운영관리자에게 긴급메시지 발송 관련 데이터가 반출되기 때문에 저속의 저비용 통신매체로 구축이 가능하다는 점이다. 다음은 이렇게 구축된 저비용 통신매체를 통해서 두 망간에는 Non-TCP/IP통신 프로토콜을 사용하여 통신한다는 점을 들 수 있다. 이는 비 보안영역내의 외부인터넷 및 기관 내 LTE모뎀 기반 빌딩시설관리 SCADA시스템 전용 외부망이 보안영역내의 빌딩시설관리 SCADA시스템 제어망을 탐지되지 않게 하기 위함이다. 즉, 비 보안영역에 존재하는 외부해커로부터 보안영역내의 빌딩시설관리 SCADA시스템을 안전하게 보호하기 위한 것이다.

3.3 빌딩 SCADA시스템 제어망과 LTE모뎀 기반 외부망간 자료전송 S/W 기능 설계

SCADA시스템 제어망 및 내부 업무망이 외부인터넷에서 활동하는 해커로부터 안전성 확보를 위해서 망간

연계 및 자료전송 S/W는『IT보안인증사무국』에서 제시한『망간 자료전송제품 보안요구사항 V1.0』을 준용하여 설계하도록 되어 있다. 이를 준용한 개략적인 전체 S/W설계는 [그림 4]와 같다. 두 망간의 자료전송은 [그림 4]에서 보듯이 보안영역인 빌딩시설관리제어망과 비 보안영역인 LTE외부망에 각각 전송통제서버를 설치하여 이들 간에만 제한적인 통신이 가능하도록 하고 있다.

이들 두 전송통제서버에 설치된 S/W의 개략적인기능을 요약하면 다음과 같다. 비 보안영역에서 가장 중요한 S/W기능은 2가지이다. 첫째는 빌딩시설관리 SCADA시스템에 반영되는 데이터는 불특정 외부사이트가 아니라 제한적인 특정사이트의 응용으로부터 유입되기 때문에 이들 사이트의 응용에서 유입되는 제어데이터만을 허용하는 기법, 즉, 화이트리스트 보안기법을 사용하여 빌딩전용 방화벽기능을 들 수 있다.

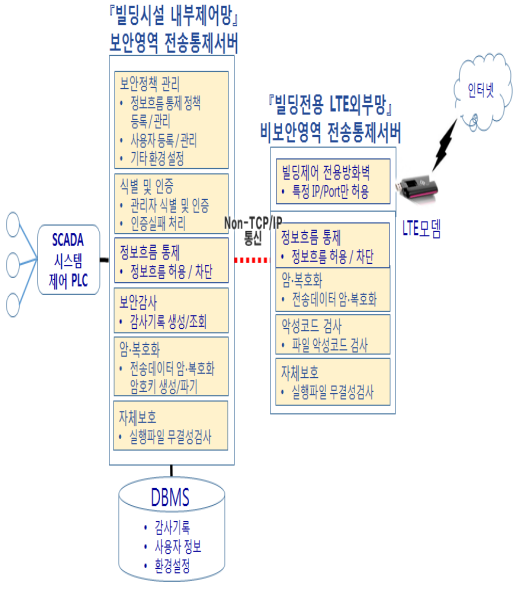

그림 4. 주요기능 S/W 기능 설계 내용

두 번째는 자유롭게 보안영역으로 정보가 흐르는 것을 통제하는 정보흐름 통제기능을 들 수 있다. 그리고 부가적인 기능으로 보안영역으로 자료전송에는 암호화가 필요하고, 악성코드 탐지 및 제거, 마지막으로 자체보호기능이 포함되어 있다. 이는 외부인터넷 해커가 제공한 악성코드/데이터들이 자유롭게 보안영역으로 침투하는 것을 막고, 악성코드를 실시간으로 감시하는 체제를 만들기 위한 것이다.

다음으로 보안영역에서 주요기능은 다음과 같다. 가장 중요한 S/W기능 중하나는 보안정책관리 기능이다. 두 망간에 안전한 자료전송 정책은 보안영역이 주가 되고 비 보안영역은 보안영역의 정책에 따라 망간 자료전송이 이루어진다. 다음으로 두 망간의 안전한 자료전송을 책임지는 관리자에 대한 식별인증기능이다. 이는 망간의 자료전송 관리 및 책임의 명확성을 위한 것이다. 다음으로 정보흐름통제 기능이다. 정보흐름통제는 보안영역의 주도하에서 이루어지도록 하고 있다. 즉, 보안영역의 요구에 따라 비보안영역의 데이터를 보안영역으로 가져오는 일방향성 자료전송을 요구하고 있다. 이는 비 보안영역에서 자유롭게 보안영역으로 데이터를 흐르게 함으로써 발생할 수 있는 해킹프로그램과 같은 악성코드의 오염을 최소화하기 위한 것으로 보인다. 기타의 S/W 기능으로는 보안감사, 암복호기능, 자체보호기능 등을 들 수 있다.

다음은 두 망간에 안전한 자료전송을 위한 보안정책 분배에 대한 기능을 설명하면 [그림 5]와 같다.

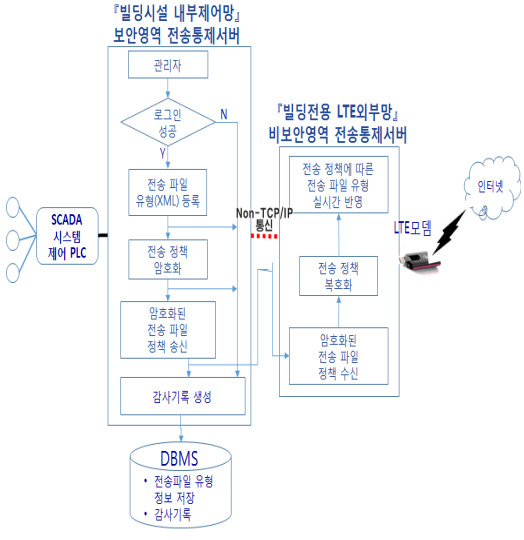

그림 5. 두 영역간에 개념적인 자료전송 보안정책 등록절차

[그림 5]에서 본 바와 같이 두 망간의 자료전송 보안정책은 보안영역의 주도하에 비 보안영역으로 정책이 시행되도록 설계되었다. 전송되는 데이터에 대해서는 모두 암호화가 필수사항이고 감사기록에는 두 망간의 자료전송에 적용된 정책과 전송파일의 유형 등이 기록된다.

마지막으로 등록된 자료전송 정책에 따른 파일 전송 절차를 살펴보면 [그림 6]과 같다.

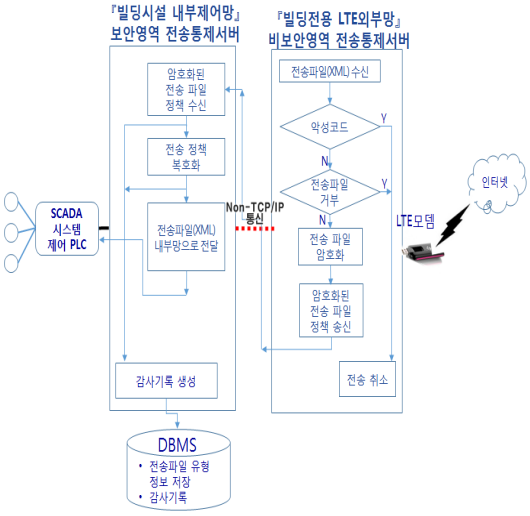

그림 6. 등록된 자료전송 정책에 따른 파일 전송절차

[그림 6]에서 보듯이 보안영역으로부터 등록된 전송파일 정책에 따라 해당되는 파일유형이 비 보안영역에 생성되면 악성코드를 검사하고, 이를 암호화하여 Non-TCP/IP통신을 통해서 보안영역으로 전송한다. 이를 수신한 보안영역은 정책에 맞은 파일인지를 검사하고 복호화 하여 내부 SCADA시스템으로 전송하는 흐름이다.

Ⅳ. 제안방안 비교 분석

이 장에서 제안한 해킹에 안전한 빌딩시설관리 SCADA시스템 제어망 구축방안이 기존의 망간 자료전송기술과 비교하여 어떤 특징을 지닌 것인지를 [표 1]에 요약하였다.

표 1. 기존 망간자료전송 기술과 비교표

망간 자료전송 비교요소	기존 망간 자료전송 기술	본 논문에서 제안한 망간 자료전송 기술
용도	일반업무망과 외부인터넷간 전송(범용)	『빌딩시설관리망』과 LTE전용외부망간 전송(전용)
망간 전송자료	범용(모든 종류 자료 대상)	전용(빌딩시설관리 SCADA 전용자료)
망간 자료전송 프로토콜	Non-TCP/IP	Non-TCP/IP
SCADA 경보체제 구축	복잡	용이 (LTE활용 스마트폰 전송)
독립적인 빌딩시설관리망 구축	불가 (빌딩 내 외부인터넷 필수)	가능 (Only LTE 외부망)
비 보안영역 전송통제서버 구축비용	고비용 (범용 PC + 인터넷 라우터)	저비용 (초소형 마이크로컴퓨터 + LTE모뎀)
비 보안영역 보안강도	약 (불특정 사이트 접근)	강 (특정사이트 접근/전용 방화벽 구축용이)

[표 1]에서 보듯이 본 논문에서 제안한 가장 유의미한 점은 빌딩시설관리 SCADA시스템 제어망에 특화된 망간 자료전송기술을 새롭게 제안한 점을 들 수 있다. 즉, 기존의 망간 자료전송기술을 빌딩시설관리 SCADA시스템에 적용할 경우 고비용, 저가용성, 구축 용이성 저하 등의 문제를 피할 수 없다는 점에 착안 한 것이다.

보다 구체적으로 주요 비교 요소별 항목에 따라 제안방안의 특이점을 정리하면 다음과 같다.

첫째, 용도측면에서 살펴보면 기존 망간 자료전송기술은 범용성이 있어 불특정 보안영역의 망에 적용이 가능하다. 반면에 제안방안은 빌딩시설관리 SCADA시스템 제어망이란 특정 보안영역의 망에만 가능하다는 점을 들 수 있다. 이는 전자의 기술이 블랙리스트기반의 보안기법을 사용한 것이기 때문이고 제안방안에서는 화이트리스트 기반의 보안기법을 사용한 결과이다. 이러한 특성 때문에 후자의 기술의 용도가 빌딩 제어망으로 한정되는 제약을 받는 반면에 화이트리스트기반 보안기술 구현 비용이 전자에 비해 파격적으로 저비용으로 구현이 가능하다는 장점을 취할 수 있다.

둘째, 망간에 전송되는 전송자료 역시 기존 기술은 불특정한 범용자료인 반면에 제안 방안에서는 특정한 제어데이터로 제한하고 있다. 이는 빌딩제어시스템에서 제어 데이터는 제한적인 종류의 정형화된 데이터라는 특성을 갖기 때문이다. 이러한 전송자료의 특성은 화이트리스트 기반의 보안기법 적용을 가능케 하여 이를 저비용으로 구현할 수 있게 한 점을 들 수 있다.

셋째, 비 보안영역의 전송 통제서버의 구축방법에서 특이점을 들 수 있다. 기존기술은 범용 PC등을 사용하여 구축한 반면에 제안기술은 초소형 마이크로컴퓨터를 LTE모뎀과 통합 패키징하여 단일 어플라이언스 형태의 제품으로 구축한 점을 들 수 있다. 이렇게 구축함으로서 기존기술과 비교하여 파격적인 초저가로 비 보안영역 전송통제서버 구축이 가능하고, 어플라이언스 형태이기 때문에 불 특정인이 장비에 접근하여 조작이 용이치 않아 보다 더 안전하고, 지리적으로 분산된 다양한 규모의 빌딩들을 대상으로 인터넷 설치와 무관하게 구축이 매우 용이하다는 특장점 등을 들 수 있다.

마지막으로 두 기술 모두 망간 자료전송 프로토콜은 Non-TCP/IP를 사용하여 보안영역에 외부 인터넷에 존재하는 해커가 직접적인 접근이 불가능하게 하였다는 점을 들 수 있다.

V. 결 론

본 논문에서 비 보안영역의 일반 외부인터넷과 보안영역의 내부 업무망 간에 적용된 기존의 망간자료전송 기술을 빌딩시설관리 SCADA시스템 제어망에 그대로 적용할 경우의 문제점을 도출하여 정리하고 이를 해결하는 방안을 제안하였다. 제안된 방안은 빌딩시설관리 SCADA시스템 제어망에 특화된 것이기 때문에 동 분야에서 기존 망간 자료전송기술을 대체할 것으로 보인다. 본 논문에서는 빌딩 제어망으로 한정했지만, 향후에는 다른 분야 SCADA시스템 제어망(전기, 수도, 수질 등)에도 그들만의 독특한 특성을 반영한 망간 자료전송 기술로 확대하여 발전시킬 필요가 있다.

참 고 문 헌

[1] “국가기관 망분리 구축 가이드,” 행정안전부, 국가정보원, 한국정보사회진흥원, 2008(5).

[2] “망간 자료전송제품 보안요구사항 V1.0,” IT보안인증사무국, 2015.

[3] 이은배, 김기영, “망 분리기반의 정보보호에대한 고찰,” 한국정보보호학회지, 제20권, 제1호, pp.39-46, 2010(2).

[4] 김경호, 장엽, 김희민, 윤정한, 김우년, “제어망 특성을 반영한 물리적 일방향 자료전달 시스템 설계,” 한국정보과학회논문지, 정보통신, 제40권, 제2호, pp.126-130, 2013(4).

[5] 이현정, 조대일, 고갑승, “망분리환경에서 안전한 서비스 연계를 위한 단방향 망간자료전송 시스템 보안모델연구”, Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, Vol.5, No.6, pp.539-547 Dec. 2015.

[6] 제어시스템 보안 국제표준 ISA/IEC 62443, https://www.isa.org

저 자 소 개

조 인 준(In-June Joe) 정회원

- 1982년 2월 : 전남대학교 계산 통계학과 학사
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
- 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

<관심분야> : 정보보호, 컴퓨터네트워크보안, 컴퓨터시스템조직응용