Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.279

에너지 기반보호시설의 보안관제 방안에 관한 연구

장 정 우,† 김 우 석, 윤 지 원‡
고려대학교 정보보호대학원

A study on the managed security services(MSS) method for energy-based SCADA Systems

Jeong-woo Jang,† Woo-suk Kim, Ji-won Yoon‡
Graduate School of Information Security, Korea University

요 약

본 연구에서는 에너지 기반보호시설 내부에서 발생 가능한 악성코드를 효과적으로 탐지 할 수 있는 네트워크 보안관제 모델을 제안하였고, 제어시스템 운영환경과 유사한 네트워크 환경에서 취득된 데이터를 상세 분석하여 보안관제시스템에 적용 가능한 탐지요소 개발과 보안관제 방안을 제시하였다. 마지막으로 시뮬레이션을 통해 제안된 네트워크 보안관제 모델이 효과적으로 이상 트래픽을 탐지 가능함을 실증하였다.

ABSTRACT

In this study, we propose an effective network managed security services model that can detect a presence of potential malicious codes inside the energy-based SCADA Systems. Especially, by analyzing the data obtained in the same environment of SCADA Systems, we develop detection factors to applicable to the managed security services and propose the method for the network managed security services. Finally, the proposed network managed security services model through simulation proved possibility to detect malicious traffic in SCADA systems effectively.

Keywords: SCADA, IDS, Firewall

I. 서 론

과거 제어시스템은 제작사 자체 소프트웨어, 하드웨어, 통신프로토콜 및 폐쇄망 구성으로 외부와 격리되어 상대적으로 보안취약성이 직접 부각되지 않았으나, 최근에는 범용의 소프트웨어, 하드웨어, 통신프로토콜의 도입과 제어시스템에서 취득된 데이터의 회사 경영정보에 활용으로 업무망 등 외부 IT시스템과의 연계에 따른 보안취약성이 크게 증가하고 있다[1],[11]. 이에 대한 대응으로 외부 연계에 따른 제어시스템의 보안취약성을 개선하기 위해 외부 연계구간에 물리적 일방향통신장치 적용을 통해 외부로부터의 공격 가능성을 원천 차단하고 있으며, 노트북이나 USB 등 외부저장매체의 부주의한 사용에 의한 악성코드 내부 유입 가능성 제거를 위해 제어시스템 컴퓨터단말에 내장된 USB포트에 대한 봉인장치 적용 등 관리적·물리적 통제를 강화하여 운영하고 있다. 그럼에도 불구하고 제어시스템의 펌웨어 업그레이드 등 성능개선이나 유지보수 목적의 휴대용 노트북이나 USB 등 외부저장매체 사용에 의해, 의도치 않은 악성코드 감염 사례가 빈번하게 발생되고 있는 추세이며 심지어 관리자조차도 제어시스템 내부 웜·바이러스 등 악성코드 유입을 제대로 인지하지 못한 채 운영하고 있는 취약한 실정이다.

접수일(2014년 11월 11일), 수정일(2015년 1월 19일), 게재확정일(2015년 2월 18일)
† 주저자, archy93@csc.motie.go.kr
‡ 교신저자, jiwon_yoon@korea.ac.kr(Corresponding author)

본 논문에서는 과거 제어시스템 이상 징후 탐지방법에 관한 수많은 선행연구가 있었으나 제어시스템 보안관제를 위해 현장 적용이 용이한 네트워크 보안관제 모델이 선행 개발되지 않은 상황을 감안하여, 산업통상자원부 산하 전력, 가스 등 에너지 기반보호시설에서 발생 가능한 악성코드를 효과적으로 탐지·방어할 수 있는 현장 상황을 고려한 네트워크 보안관제 모델을 제안하고 현장에서 취득된 데이터를 분석하여 보안관제시스템에 적용 가능한 탐지요소를 개발하였다. 마지막으로 실제 제어시스템 운영 환경과 유사한 시뮬레이션 환경을 구성하고 개발된 탐지요소를 네트워크 보안관제 모델에 적용하여, 과거 에너지 기반보호시설에서 발생되었던 네트워크 웜·바이러스나 서비스거부공격 등 유해환경을 임의 발생시켜 제안된 네트워크 보안관제 모델이 효과적으로 이상 징후 탐지 가능함을 실증하였다.

II. 관련 연구

네트워크 기반의 침입탐지시스템(IDS : Intrusion Detection System)은 관제를 용이하게 하고 알려진 공격에 대해 높은 탐지율을 보이기 때문에 보안관제용 설비로 주로 활용되고 있다[2],[3].

일반적으로 제어시스템에서 발생 가능한 사이버 위협을 탐지하기 위한 방법에는 이상행위기반 탐지(anomaly detection)와 시그니쳐기반 탐지(misuse detection) 그리고 화이트리스트기반 탐지 등으로 크게 구분할 수 있다[4],[5],[6].

화이트리스트 탐지방법은 제어시스템에서 발생되는 모든 행위를 화이트리스트의 프로파일로 정의하고 정의된 서비스 외 모든 행위를 제한하는 방법으로 제어시스템의 가장 이상적인 탐지방법으로 연구되고 있다.

그러나 국내 운영중인 에너지분야 기반보호시설은 대부분 해외 메이저 제작사가 개발하여 수십년전 도입된 구형시스템으로 화이트리스트 프로파일 생성에 필요한 개발문서의 미비와 해외 제조사의 기술지원 등 신속한 협조체계에 한계가 있어 완벽한 화이트리스트 프로파일을 생성하는 것이 현실적으로 어려운 측면이 있다.

무엇보다 제어시스템은 무중단과 상시적인 가용성을 최우선으로 확보해야 한다는 측면에서, 향후 신규 제작·도입되는 설비에 대해서는 화이트리스트 탐지방법의 시스템 적용 가능성이 충분하리라 판단되지만, 현재 운영중인 에너지 기반보호시설에서는 직접 적용하기 어렵다는 실무적인 판단하에 본 논문에서는 화이트리스트 탐지방법에 대한 실증을 별도로 다루지 않았다.

2.1 이상행위(Anomaly)기반 탐지 방법론

이상행위기반 탐지방법은 네트워크상의 트래픽이나 시스템 자원의 사용이 정상적인 범주를 벗어나는 경우를 탐지하는 방법론이다. 이 방법은 제로데이 공격(zero-day attack)과 같은 알려지지 않은 취약점을 이용한 공격이나 정보보호시스템을 우회하여 탐지되지 않는 지능적이고 새로운 공격까지도 탐지 할 수 있는 장점이 있다.

일반적으로 제어시스템에 대한 공격패턴이 거의 알려져 있지 않은 사이버위협 상황에서는 이상행위 탐지를 수행하는 것이 더 적합하게 고려되어 최근의 제어시스템 보안을 위한 많은 연구에서 활용되고 있다. 그러나 시스템 구현에 어려움이 있고, 기존 이상행위 탐지 방식의 단점인 대량의 보안 이벤트 상에서 오경보(False Alarm)를 분류해야 한다는 문제점과 이상 징후 탐지 후 수작업으로 어떤 공격이 발생되었는지 상세 분석하는 과정이 필요하다는 점 그리고 정해진 정상적인 범주 내에서 발생되는 공격을 탐지하지 못한다는 문제점은 여전히 남아 있다[1],[7].

2.2 시그니쳐(Signature)기반 탐지 방법론

시그니쳐기반 탐지방법은 오용 탐지(misuse detection)라고도 하며 시그니쳐 혹은 패턴을 이용하여 매치되는 모든 알려진 공격을 탐지하는 방법론이다. 이 방법은 패턴으로 정의된 모든 알려진 공격을 정확히 탐지 할 수 있는 장점이 있으나, 일반적으로 제어시스템에 대한 공격패턴이 거의 알려져 있지 않은 사이버 위협 상황에서는 탐지가 어렵고, 무엇보다 제로데이 공격(zero-day attack)과 같은 새로운 형태의 공격에 대해서는 상세분석을 통해 탐지패턴을 지속적으로 개발하여 시스템에 적용하기 전까지는 탐지가 불가능하다는 문제점이 존재한다. 따라서 최근의 산업제어시스템에 적용하기에는 다소 한계가 존재하는 탐지 방법론이다.

III. 현재 상황 및 보안 위협

제어시스템에서 취득된 데이터의 회사 경영정보 활용 등 외부 IT시스템과의 연계 필요성 증가에 따른 공격자의 제어시스템 접근성 향상으로 제어시스템 해킹 위험성은 꾸준히 증가하고 있다. 미국 국토안보부(DHS : Department of Homeland Security)

산하 산업제어시스템 사이버위기대응팀(ICS-CERT) 사이버공격동향보고서에 따르면 기반시설에 대한 사이버공격이 주로 에너지 분야에 집중되고 있으나, 제조시설, 통신시설, 수자원관리시설, 교통시설 등으로 광범위해지고 있으며, 사이버공격 규모가 확대되고 있을 뿐만 아니라 공격의 정교함과 속도 역시 상승하고 있음을 지적하고 있다[8].

국내 에너지 기반보호시설은 외부와의 연계 접점 구간을 안전한 자료연계 방식의 하나인 물리적일방향 통신장치 등을 이용하여 외부의 침입 가능성을 원천 차단하였으나, 유지보수나 성능분석 등 자료 취득 필요성으로 인한 노트북이나 USB 등 외부저장매체의 무분별한 사용으로 악성코드 감염사례가 종종 확인되고 있으며, 최근 다양한 해외 제어시스템 사고사례[9],[10]에서 보듯이 제어시스템은 더 이상 안전지대가 아님이 증명되고 있다. 무엇보다 지금까지의 국내 에너지 기반보호시설에 대한 보안관리정책은 주로 관리적·물리적 접근통제방법에 치중하여 운영되고 있으며, 제어시스템 내부 트래픽에 대한 이상 징후를 실시간 탐지할 수 있는 네트워크 보안관제 모델이 확립되지 않은 실정이다.

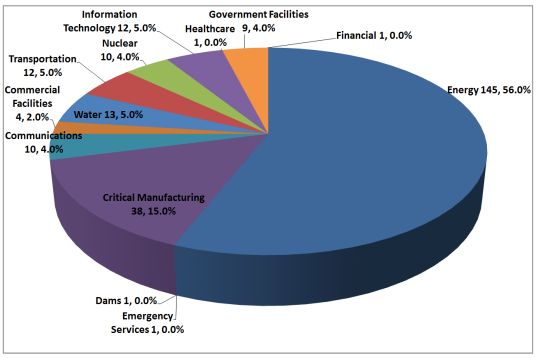

Fig. 1. 2013 ICS-CERT year in review[8]

IV. 제안하는 보안관제 모델

국내 산업통상자원부 산하 에너지 기반보호시설은 2014년 09월 기준, 9개 기관 37개 시설을 운영하고 있으며, 네트워크 구성 측면에서는 크게 타 지역에서 원격제어가 가능한 전국단위의 광역망 구성의 기반보호시설과 단일지역에서만 제어가 가능한 단일망 구성의 기반보호시설로 구분할 수 있다.

망 구성별 악성코드 등 유해트래픽을 효과적으로 탐지·대응하기 위해서는 감시 및 제어용 데이터가 송·수신되는 네트워크 접점구간에 보안시스템을 구축하는 것이 관건이라 할 수 있다. Table 1은 광역망과 단일망 구성 제어시스템의 보안측면에서 특성을 비교한 내용이다.

Table 1. Comparing characteristics of wide and local area SCADA Systems

Division	Wide Area SCADA Systems	Local Area SCADA Systems
Redundancy	Local and remote backup and redundancy	Local backup and redundancy
Remote Control	Remote data acquisition and control in emergency	Manual operation by control panel in emergency
Damage ranges	Wide damage through dedicated line	Restrictive damage in local
Manufacturer	Domestic	Foreign
Technical Support	Easy	Difficulty

4.1 광역망에서 일반구성 및 운영방법

전국 단위의 광역망으로 구성된 에너지 기반보호시설은 상위사업소와 하위사업소간 전용회선으로 연계되어 하부사업소에서 취득되는 모든 데이터를 상위사업소로 전달하는 계층구조로 되어 있다. 산업통상자원부 산하 에너지 기반보호시설은 한국전력공사의 송변전스카다시스템, 배전지능화시스템 등이 있으며, 한국가스공사의 천연가스배관망감시제어시스템, 한국전력거래소의 전력계통운영시스템이 있다.

일반적으로 기반보호시설 운영기관의 운영방법에 따라 다소 차이는 존재하지만, 광역망에서 기반보호시설의 운전은 상위사업소에서 현장 데이터 계측이나 제어를 통합 관리하도록 되어 있으며, 상위사업소의 천재지변이나 시스템 장애 등의 원인으로 정상적으로 운영하기 어려운 상황에서는 제어권을 원격지의 하위사업소로 이양하여 24시간 무중단 시스템 운영이 가능하도록 이중화되어 있다.

4.2 광역망에서 보안관제 모델

광역망에서는 상위사업소에서 직할과 원격지 하위

사업소의 제어시스템 계측이나 제어를 동시에 수행 가능한 네트워크로 구성되어 있다. 일례로 상위사업소에 위치하고 있는 운전원이 직할 제어시스템을 제어하게 되면 해당시스템이 직접 연결되어 있는 네트워크 스위치로 모든 제어용 데이터가 유입되고, 원격지의 하위 사업소 제어시스템의 계측이나 제어를 수행하게 되면 운영에 필요한 모든 데이터는 전용회선을 통과하게 되어 있다. 이처럼 광역망에서 제어용 데이터 흐름과 네트워크 구성을 이해하고 광역망 기반보호시설에서 발생되는 보안이벤트를 수집하여 보안관제시스템에 활용하기 위해서는 Fig.2와 같이, 제어용 트래픽이 유입되는 최적의 네트워크 구간에 이상 트래픽 탐지가 가능한 보안시스템을 배치하여야 하며, 본 논문에서는 보안관제시스템으로 가장 활용도가 높은 침입탐지시스템(IDS)과 침입차단시스템(firewall)을 이용한 보안관제 모델을 제안하였다.

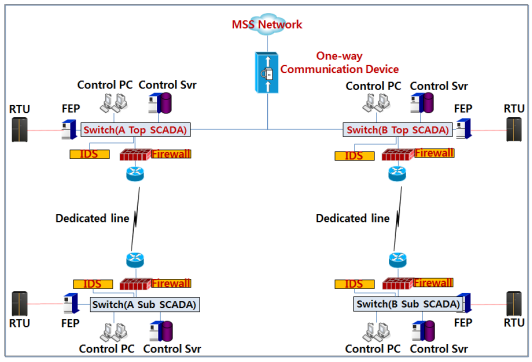

Fig. 2 Managed security services applicable model in wide area SCADA Systems

4.2.1 침입탐지시스템(IDS) 적용 방법

국내 에너지 기반보호시설의 업무망간 연계접점은 국가사이버안전센터의 “국가 기반시설 전자제어시스템 보안가이드라인”을 준용하여 물리적인 일방향통신장치 등으로 안전하게 구성되어 있으며, 외부에서 해킹이나 악성코드 유입이 어려운 네트워크 환경이다.

일반적으로 에너지 기반보호시설로 악성코드가 유입될 수 있는 주요 원인은 신뢰성이 검증되지 않은 비인가 USB 등 외부저장매체를 제어용 컴퓨터단말에 연결하는 것으로 야기된다. Fig.3에서 보는바와 같이 운전단말, 주장치서버, FEP 등 제어시스템을 구성하는 주요 컴퓨터단말은 네트워크 스위치에 직접 연결되어 있으며, 비인가 USB 등의 외부저장매체를 이용한 최초의 악성코드 유입이 예상되는 컴퓨터단말에서 발생되는 모든 트래픽을 수집하여 침입탐지시스템으로 주입 가능한 네트워크 구성이 되어야 효과적으로 제어시스템 내부에서 발생되는 이상 트래픽의 탐지가 가능하다. 대부분의 에너지 기반보호시설의 제어용 컴퓨터단말이 연결된 네트워크 스위치는 단순 Layer2 구성으로 되어 있으며, 이중화된 네트워크 주·예비 스위치에 연결된 컴퓨터단말의 모든 물리적 통신포트에서 발생되는 트래픽을 수집하여 침입탐지시스템으로 주입하기 위해서는 port-mirroring 기술을 이용하여 구현 가능하다.

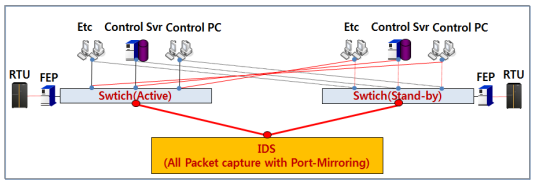

Fig. 3. IDS applicable model in wide area SCADA Systems

4.2.2 침입차단시스템(Firewall) 적용 방법

광역망에서 침입차단시스템은 네트워크 연계구간설치되어 허용된 트래픽만 전송하고 그 외 허용되지 않은 모든 트래픽에 대한 외부 유·출입을 차단하는 역할을 수행한다. 광역망에서 제어시스템 보안관제를 위해서는 침입탐지시스템을 이용한 네트워크 스위치에서 발생되는 직할 트래픽에 대한 탐지뿐 만아니라, 직할이나 원격지에서 유·출입되는 트래픽에 의해 발생되는 허용되거나 거부되는 보안로그를 활용한 행위분석이 가능하다.

4.2.3 관제망으로 안전한 보안로그 전송 방법

본 연구에서 광역망 에너지 기반보호시설의 보안관제를 위해 최소 필요 보안설비로 제안한 침입탐지시스템 및 침입차단시스템에서 생성된 보안이벤트를 제어시스템과 격리된 관제망으로 안전하게 전송하기 위해서는 국가사이버안전센터의 “국가 기반시설 전자제어시스템 보안가이드라인”을 준용한 방식으로 전송하여야 하며, Fig.4와 같이 에너지 기반보호시설에서는 외부에서 원격 접근이 원천적으로 불가능한 일방향통신장치나 Non-TCP/IP기반 공유 스토리지 전송시스템을 이용한 네트워크 구성으로 연계한다.

일반적으로 침입탐지시스템은 탐지포트와 관리포트가 물리적으로 격리된 시스템 특성으로 관리포트를 관제망에 직접 연결하여 보안이벤트 전송이나 탐지룰 업데이트를 시행하고 침입차단시스템은 제어시스템 내부에 설치되는 구조적 특성으로 인해 광역망에서 발생되는 모든 보안로그를 최상위사업소의 통합로그수집서버로 집중한 후, 이를 다시 일방향통신장치를 경유하여 관제망으로 데이터를 전송하여 제어시스템 보안관제로 인한 새로운 보안취약점이 발생되지 않도록 구성하여야 한다.

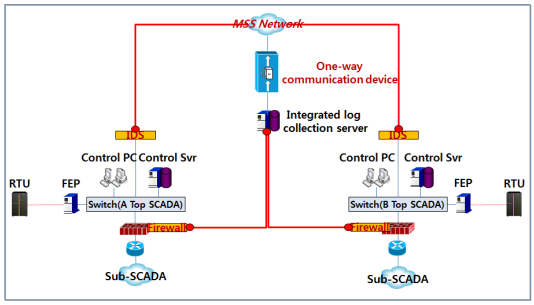

Fig. 4. Transport model of security log for managed security services network

4.3 광역망에서 악성코드 확산방지 대책

광역망 에너지 기반보호시설은 전용회선을 통해 상호 유기적으로 연계되어, 비상 상황 시 원격지에서 신속한 원격제어가 가능하여 제어시스템의 가용성을 극대화 할 수 있는 장점이 있지만, 부주의한 운영관리로 인해 악성코드의 유입 시 원격지로 피해가 확산 될 수 있는 단점이 존재한다. 유해 트래픽 확산에 의한 광역망 단절을 방지하기 위해서 악성코드가 최초 유입된 직할에서 유해 트래픽이 원격지로 확산되지 않도록 침입차단시스템 등 운영설비의 보안설정을 강화하여야 한다.

4.3.1 침입차단시스템 보안정책 적용 방법

최초 악성코드가 유입된 직할에서 전용회선을 이용한 타 사업소로 피해가 확산되는 것을 방지하기 위해서 침입차단시스템을 이용한 대응이 필요하다. 침입차단시스템에서는 상위사업소와 하위사업소간 서비스 허용이 필요한 보안정책만을 허용하고, 나머지 트래픽에 대해서는 차단 적용한다. 최적화된 침입차단시스템의 표준보안정책을 적용하기 위해서는 상위사업소와 하위사업소간 통신 시 필요한 서비스를 개발문서 등을 활용하여 사전 분류하여야 하며, 일반적으로 침입차단시스템의 보안정책 적용 시 최소한의 IP, Port로 제한한다.

4.3.2 네트워크 스위치 보안설정 방법

무분별하게 생성된 네트워크로 다량의 유해트래픽을 확산시키는 네트워크 웜·바이러스는 네트워크 설비의 default-gateway설정에 의해 상위사업소로 확산될 수 있다. 네트워크 웜·바이러스에 의한 다량의 유해트래픽 유입으로 전용회선의 트래픽 폭주에 따른 제어명령의 지연이나 시스템 자원소모에 따른 서비스 거부공격이 유발될 수 있으며, 이를 개선하기 위해서는 광역망에서 사전 정의되지 않은 IP대역으로 전송되는 트래픽에 대해서는 'null 0'라는 가상 인터페이스로 패킷을 포워딩하여 폐기시키는 null- routing을 적용한다.

4.4 단일망에서 일반구성 및 운영방법

단일망으로 구성된 에너지 기반보호시설은 운영기관이나 다양한 시스템 제조사에 따라 다소 상이한 네트워크 구성이 존재하지만, 본 논문에서는 에너지 기반보호시설의 대부분을 점유하고 있는 발전제어시스템의 일반적인 시스템 구성을 토대로 단일망에서 네트워크 보안관제 모델을 제안하였다.

4.5 단일망에서 보안관제 모델

단일망을 구성하고 있는 발전제어시스템은 발전소(호기)별 제어시스템이 물리적·기능적으로 독립 운전되는 네트워크 구성으로 되어 있다. 일례로 운전원이 운전단말을 이용하여 제어시스템을 조작하게 되면 시스템이 연결되어 있는 네트워크 스위치로 모든 제어용 신호가 전달되고, 이를 통해 주장치서버 등을 경유하여 최종적으로 하부의 밸브나 모터와 같은 현장 필드장치가 조작되게 된다. 단일망 에너지 기반보호시설의 운용 특성을 고려하여 제어시스템에서 발생되는 보안이벤트를 수집하여 보안관제에 활용하기 위해서는 Fig.5와 같이 제어용 데이터가 유입되는 최적의 네트워크 구간에 이상 트래픽 탐지가 가능한 보안시스템을 배치하여야 한다.

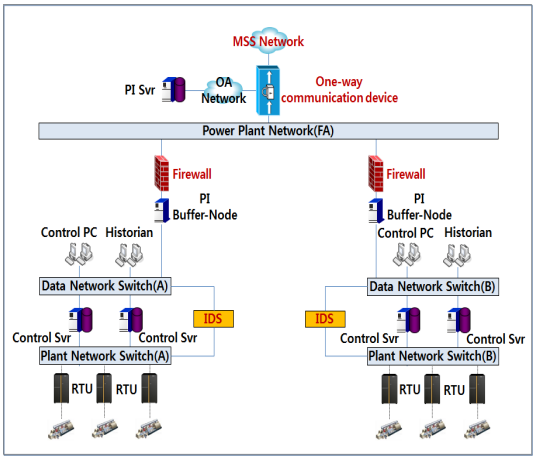

Fig. 5 Managed security services applicable model in local area SCADA Systems

4.5.1 침입탐지시스템(IDS) 적용 방법

Fig.6은 특정 호기의 발전제어시스템 네트워크 이중화 구성을 상세히 도식화 한 것으로 운전단말, 주장치서버, Historian 등 발전제어시스템을 구성하는 주요 컴퓨터단말은 네트워크 스위치에 연결되어 있으며, 비인가 USB 등의 외부저장매체를 이용한 최초의 악성코드 유입이 예상되는 컴퓨터단말에서 발생되는 모든 트래픽을 수집하여 침입탐지시스템으로 주입 가능한 네트워크 구성이 되어야 효과적으로 제어시스템 내부에서 발생되는 이상 트래픽의 탐지가 가능하다. 단일망의 에너지 기반보호시설의 제어용 컴퓨터단말이 연결된 네트워크는 단순한 Layer2 구성으로 되어 있으며, 이중화된 네트워크 주·예비 스위치의 모든 물리적 통신포트에서 발생되는 트래픽을 수집하기 위해서는 네트워크기반 port-mirroring 기술을 적용하여 침입탐지시스템으로 주입 가능하다.

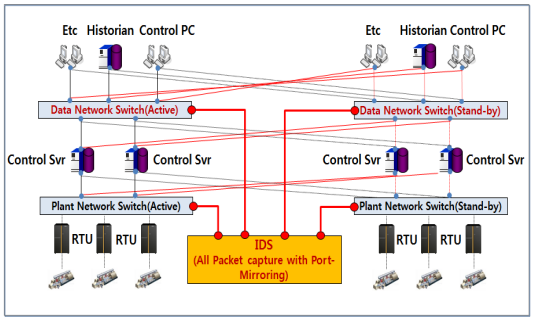

Fig. 6. IDS applicable model in local area SCADA Systems

4.5.2 침입차단시스템(Firewall) 적용 방법

광역망 네트워크 보안관제 모델에서 침입차단시스템은 타 사업소로 유해 트래픽 확산 방지 역할을 수행하였으나, 단일망의 발전제어시스템에서 침입차단시스템 역할은 발전소(호기)별 네트워크 격리를 위한 용도로 활용된다. Fig.7과 같이 물리적으로 완전 독립되어 운영중인 발전소(호기)별 제어시스템은 운전정보(PI)의 회사 경영정보 활용으로 상위 네트워크 구간인 발전전용망(FA)에서 통합 연계되고 있으며, 이로 인해 특정 발전소(호기) 제어시스템에서 악성코드 유입 시 발전전용망을 통해 직할의 타 발전소 제어시스템으로 피해 확산이 가능한 구성 취약점이 존재한다. 이에 대한 방지대책으로 발전소(호기)별 상위 연결 네트워크 접점구간에 침입차단시스템을 적용하여 발전소(호기)별 네트워크 격리를 유지하면서 관제망으로 안전하게 데이터를 전달하도록 구성한다.

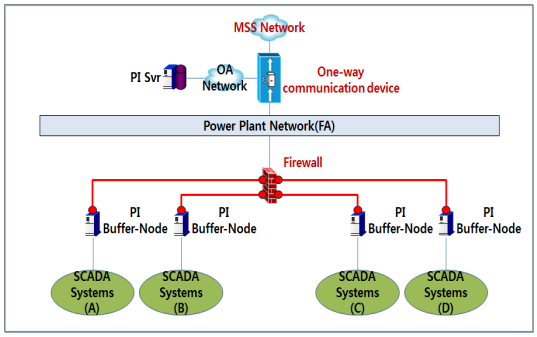

Fig. 7. Firewall applicable model in local area SCADA Systems

4.5.3 관제망으로의 안전한 보안로그 전송 방법

단일망 에너지 기반보호시설의 보안관제 수행을 위해서는 "4.2 광역망에서 관제망으로 안전한 보안로그 전송방법"을 준용한 방식으로 전송한다.

Fig.8와 같이 침입탐지시스템은 관리포트를 관제망으로 직접 연결하여 보안이벤트 전송이나 탐지룰 업데이트를 안정적으로 수행하고, 침입차단시스템은 일방향통신장치를 경유 후, 전송하여 제어시스템 보안관제로 인한 새로운 보안 취약점이 발생되지 않도록 구성한다.

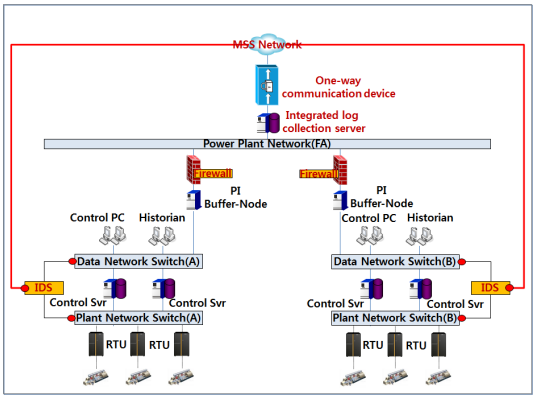

Fig. 8. Transport model of security log for managed security services network

V. 데이터 상세 분석 및 탐지요소 개발

본 연구에서 에너지 기반보호시설의 보안관제 시, 최소 필요 보안설비로 제안한 침입탐지시스템과 침입차단시스템을 이용하여 광역망에서 정상 동작 범위를 벗어나는 비정상 행위기반 탐지요소 개발을 위해 침입차단시스템의 허용·거부 보안로그를 활용하였다. 그리고, 단일망과 광역망을 모두 포함하는 직할 구간에서 중요 제어명령의 실행이나 위·변조 상황을 실시간 모니터링 할 수 있는 시그니쳐기반 탐지룰 개발을 위해 실제 운전환경과 유사한 현장용 시뮬레이터에서 데이터를 취득하였다.

5.1 행위기반 탐지요소 개발을 위한 데이터 취득분석

광역망 네트워크 보안관제 모델을 대상으로 제어시스템이 운영되는 시스템 환경과 유사한 독립 폐쇄망에서 Fig.9와 같이, 상위사업소 네트워크 접점구간에 위치하는 침입차단시스템에서 실시간 송·수신되는 보안로그를 24시간 취득·분석하였으며, 상세내용은 Table 2와 같다. 일반적으로 침입차단시스

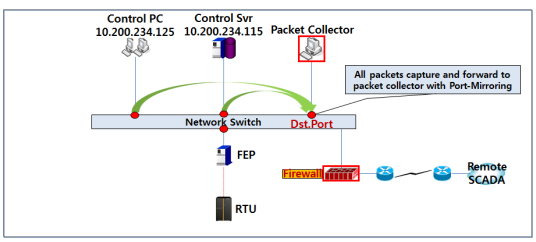

Fig. 9. Data acquisition model in field

Table 2. Firewall's acquisition data summary in wide area SCADA Systems

Division	Detailed Description					
Data acquisition period	2014.03.01. 00:00 ~ 24:00					
Security log count	Time	Count	Time	Count	Time	Count
	00~01	5,675	01~02	5,676	02~03	5,766
	03~04	4,286	04~05	4,333	05~06	4,274
	06~07	4,367	07~08	4,803	08~09	4,735
	09~10	5,784	10~11	6,561	11~12	6,780
	12~13	6,436	13~14	7,171	14~15	6,953
	15~16	6,408	16~17	6,972	17~18	7,010
	18~19	6,909	19~20	6,298	20~21	6,656
	21~22	6,489	22~23	7,014	23~24	5,717
Average security log count	5,961					
Total security log count	143,073					

템에서 생성되어 보안관제시스템으로 Syslog 포맷 전송 가능한 보안로그 객체는 출발지IP, 목적지IP, 목적지Port, 사용프로토콜, 전송량, 수신량, 유지시간 등으로 분류할 수 있으며, 본 논문에서는 취득된 광역망 침입차단시스템의 보안로그를 분석하여 보안관제시스템의 활용 가능한 탐지요소를 개발하였다.

Table 3. Allowance syslog format of Firewall

Division	Log Admitted	Time	UI	Src.IP	Src. Port	Protocol
	Dst.IP	Dst. Port	Snd. Bytes	Rcv. Bytes	Duration	Interface

5.1.1 출발지 및 목적지 IP주소

실제 측정 데이터 분석결과, Fig.10와 같이 정상

운전 상황에서는 내부시스템에 사전 정의된 IP주소로 형성된 IP세션이 5개 확인되었으며, 그 외 비정형 IP 세션의 보안로그는 검출되지 않았다.

정상 통신을 가장한 지능화된 공격탐지에 대해서는 추가적인 고려가 필요하지만 일반적인 네트워크 웜·바이러스와 같이 무작위 네트워크를 임의 생성하여 유해 트래픽을 다량 발생시키는 악성코드의 제어 시스템 유입 시, 이상 징후를 확인할 수 있는 탐지요소로 활용 가능함을 확인하였다.

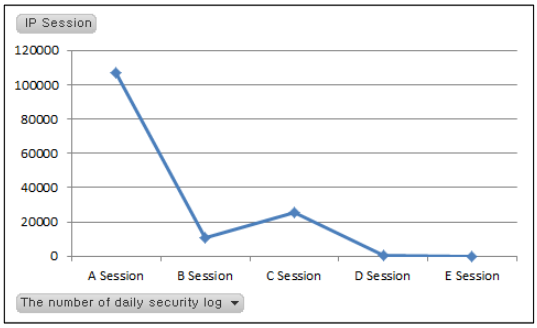

Fig. 10. Source and destination IP session distribution of the security log

5.1.2 목적지 포트

제어시스템의 상호 설비별 동작을 위해 개발 시 어플리케이션 레벨에서 사전 정의된 서비스 포트는 변화가 존재하지 않아 이상 징후 탐지를 위한 보안관제시스템에 활용 가능한 탐지요소중의 하나이다.

실제 취득된 데이터에서도 Fig.11에서 보는바와 같이, 목적지 포트의 분포는 7건으로 일정한 규칙성이 존재함을 확인하였으며 이를 통해 사전 정의된 목적지 포트를 벗어나는 접속에 대해서는 비정상행위로 분류하여 탐지 가능함을 확인하였다.

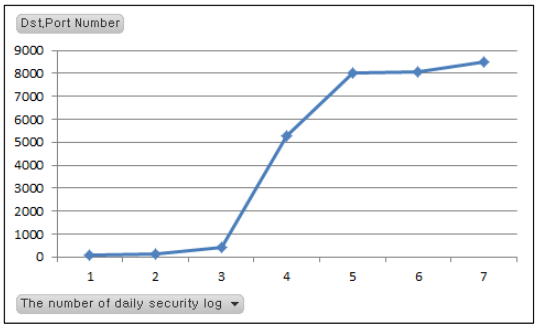

Fig. 11. Destination port distribution of the security log

5.1.3 송신 데이터량

실제 취득된 데이터 분석결과, Fig.12에서와 같이 송신 데이터량의 분포가 최소 70bytes에서 최대 941,082bytes로 10,506건의 지나치게 광범위하고 일정한 규칙성이 존재하지 않아 보안관제시스템에서 이상 징후를 판단하는 탐지요소로 활용하기에는 어려움이 있음을 확인하였다.

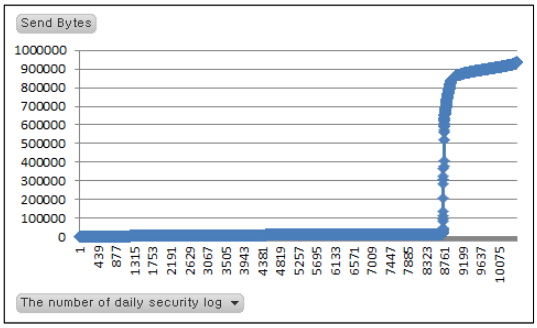

Fig. 12. Send bytes distribution of the security log

5.1.4 수신 데이터량

실제 취득된 데이터 분석결과, Fig.13에서와 같이 수신 데이터량의 분포가 최소 0Bytes에서 최대 38,576Bytes로 1,330건의 지나치게 광범위하고 일정한 규칙성이 존재하지 않아 보안관제시스템에서 이상 징후를 판단하는 탐지요소로 활용하기에는 어려움이 있음을 확인하였다.

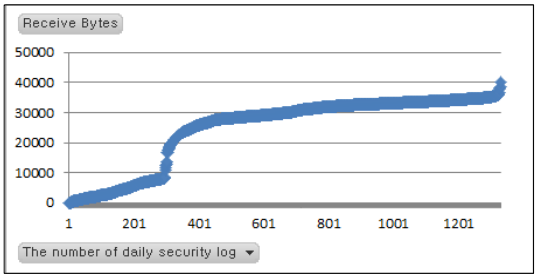

Fig. 13. Received bytes distribution of the security log

5.1.5 유지시간(Duration)

침입차단시스템에서 유지시간은 설비별 상호 데이터 송·수신을 위해 일정시간 통신이 유지되는 시간을 의미한다. 실제 취득된 데이터에서 보안로그의 유지시간은 Fig.14에서와 같이 최소 3ms에서 최대 4,401ms까지 47건으로 상대적으로 IP주소나 목적지 포트에 비해 불규칙한 특성을 가지고 있음을 확인하였으며, 로그수집 기간을 길게 할수록 분포가 넓어져 보안관제시스템에서 이상 징후를 판단하는 탐지요소로 활용하기에는 어려움이 있음을 확인하였다.

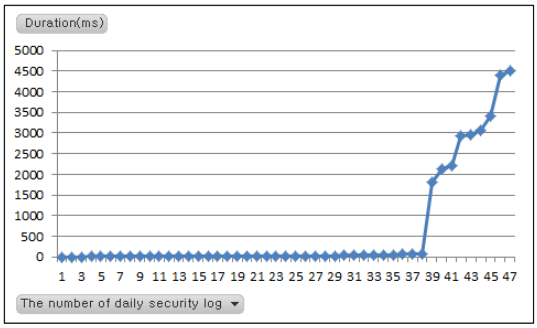

Fig. 14. Duration distribution of the security log

5.1.6 프로토콜

침입차단시스템의 보안로그에서 확인 가능한 프로토콜은 TCP, UDP, ICMP로 크게 분류 가능하며, 이는 범용 TCP/IP기반 통신방식의 특성을 나타내는 것으로 제어시스템만의 이상 징후를 판단하는 탐지요소로 활용하기에는 한계가 존재함을 확인하였다.

실제 취득 데이터를 이용한 상세 분석결과, 이상 징후 탐지를 위해 보안관제시스템의 탐지요소로 활용 가능한 침입차단시스템의 보안로그 객체는 출발지·목적지 IP주소, 목적지 포트로 분류되었으며, 사용 프로토콜, 송·수신 데이터량, 유지시간 등 그 외 보안로그 객체의 탐지요소 활용에는 해당 제어시스템에 대한 추가적인 검토가 필요함을 확인하였다.

5.2 시그니쳐기반 탐지룰 개발을 위한 데이터 취득분석

중요 제어명령의 실행이나 위·변조를 실시간 탐지할 수 있는 시그니쳐기반의 탐지룰 개발을 위해 Fig.9와 같이, 국내 에너지 기반보호시설에서 사용중인 현장용 시뮬레이터를 이용하여, 운전단말에서 현장단말장치(RTU) 제어를 위한 열림/닫힘 제어명령 실행 시 주장치서버와 FEP으로 전달되는 모든 데이터를 패킷분석툴을 이용하여 수집하였다. 현장 필드장치에 대한 실제 제어명령 실행 시 제어시스템 운전 및 가용성에 큰 영향을 미칠 수 있는 중요 제어명령을 분류하여, 침입탐지시스템에서 중요 제어명령에 대한 실행이나 위·변조를 실시간 탐지할 수 있는 시그니쳐기반 탐지룰 개발 방향성 제시를 목표로 하였다. 이를 위해 국내 에너지 기반보호시설에서 운용중인 현장용 시뮬레이터를 이용하여 운전단말에서 현장 필드장치 제어를 위한 열림/닫힘 제어명령 실행 시, 주장치서버와 FEP장치로 전달되는 패킷을 일정시간 수집·분석하였으며 수집된 패킷의 요약은 Fig.15와 같다.

Protocol	% Packets	Packets	% Bytes	Bytes
Frame	100.00 %	40384	100.00 %	5712758
Ethernet	99.81 %	40307	99.88 %	5705828
Internet Protocol Version 4	94.44 %	38139	97.36 %	5562119
Transmission Control Protocol	93.79 %	37876	96.87 %	5534220
General Inter-ORB Protocol	68.92 %	27833	66.00 %	3770259
Text item	68.92 %	27833	66.00 %	3770259
Cosnaming Dissector Using GIOP API	0.02 %	9	0.03 %	1831
Data	1.88 %	758	5.67 %	323808
Short Message Peer to Peer	0.01 %	3	0.07 %	4258

Fig. 15. Collected data summary of simulator

수집된 패킷의 사용 프로토콜 분석 결과, 현장 필드장치의 열림/닫힘 명령 등 제어시스템 운전에 사용되는 프로토콜은 전체 IP(94.44%)에서 대부분 TCP(93.79%)인 것으로 확인되었다. 현장 필드장치의 열림/닫힘 실행에 직접 연관된 명령코드를 확인하여 침입탐지시스템에 적용 가능한 시그니쳐를 개발하기 위하여, 운전단말에서 열림/닫힘 실행 시 발생되는 패킷(Push, Ack)을 집중 수집하였으며, 이를 통해서 현장 필드장치 열림/닫힘에 관여하는 패킷을 특정할 수 있었다.

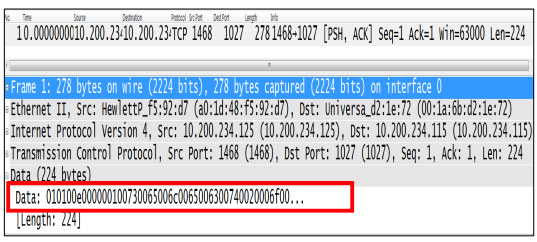

Fig. 16. Open-command's payload of field device

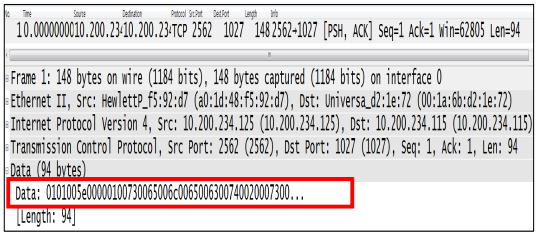

Fig. 17. Close-command's payload of field device

현장 필드장치 제어에 관여하는 문자열을 추출하여 제어시스템의 가용성에 직접 영향을 미치는 열림/닫힘과 같은 중요 제어명령 실행이나 위·변조 상황을 실시간 모니터링하기 위하여 Table 4와 같이 침입차단시스템에 적용 가능한 Snort룰을 제작하였다.

일반적으로 제어시스템의 중요 제어명령 실행이나 위·변조에 따른 이상 징후 탐지를 위해서는 중요 제어명령을 분류하고, 시그니처기반 탐지룰 제작이 필요한 제어명령에 대해서는 지속적으로 탐지룰을 제작하고 관리할 수 있는 내부 업무 프로세스를 유지하여야 한다. Fig.18은 중요 제어명령에 대한 탐지룰 제작 프로세스를 도식화하였다.

Table 4. Detection signature and name for detecting of control-command

Division	Detection signature	Detection name
Open -Control	alert tcp any any <> any 1027 (content:"|010100e000000100|"; offset: 0; depth: 8;)	attack-scada-control(open).14101602@motiecsc
Close -Control	alert tcp any any <> any 1027 (content:"|0101005e00000100|"; offset: 0; depth: 8;)	attack-scada-control(close).14101601@motiecsc

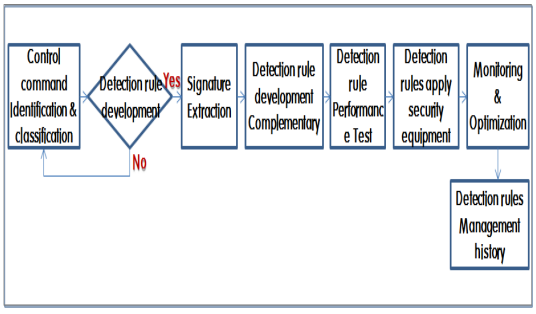

Fig. 18. Development process for detection rules in general

현장용 시뮬레이터를 이용한 실제 취득 데이터 상세 분석결과, 에너지 기반보호시설의 가용성에 심각한 영향을 미칠 수 있는 중요 제어명령에 대한 이상 징후 탐지를 위해 중요 제어명령에 대한 탐지룰을 개발하고 이를 침입탐지시스템에 적용하여 실시간 모니터링이 가능하다는 점을 실증하였다.

VI. 시뮬레이션 실증

6.1 환경 구축

제안된 네트워크 보안관제 모델에서 침입탐지시스템과 침입차단시스템이 변화된 이상 징후를 효과적으로 탐지 가능함을 실증하기 위해, 에너지 기반보호시설의 보안관제 방향성으로 제시된 네트워크 보안관제 모델과 유사한 시뮬레이션 환경을 구성하였다.

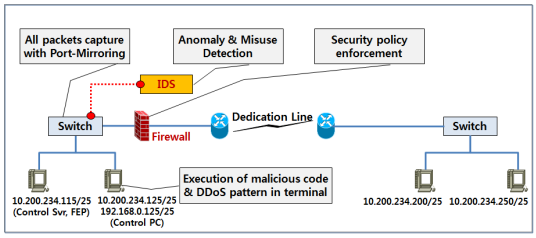

Fig. 19. Simulation model in wide area SCADA Systems

Table 5. Simulation component

Division		Manufacturer	Model	O/S
Firewall		Wins	E-2000	Secu O/S
IDS		Secui	NXG-200	Secu O/S
Network Protocol Analyzer		Wireshark	Wireshark	v1.12.1
Terminal		HP	8530P	Win 7
Network	Router	Cisco	C-1821	IOS
	Switch	Cisco	C-2920	IOS
Attack Pattern	Control Execution	• Open & Close-control		
	UDP Flooding	• DDoS Pattern Generator (Unicorn)		
	ICMP Flooding	• ICMP Flooding Generator		
	Network Malicious Code	• Random Traffic Generator (SolarWinds Toolset)		

6.2 실증

네트워크 보안관제 모델로 제시된 네트워크 구성과 유사한 시뮬레이션 환경을 구축하여 중요 제어명령의 실행과 내부의 네트워크 웜·바이러스나 서비스 거부공격과 같은 유해 트래픽 유입 시, 제5장에서 개발된 침입탐지시스템의 시그니쳐기반 탐지룰과 침입차단시스템의 행위기반 탐지요소를 활용하여 효과적으로 탐지 가능함을 확인하였다. 에너지 기반보호시설과 유사한 시뮬레이션 환경에서 내부의 이상 징후 탐지를 위하여 네트워크 스위치의 port-mirroring 기술을 활용하여 침입탐지시스템으로 모든 패킷을 주입시켰다. 또한, 중요 제어명령에 대한 실행 등 이상 징후 탐지 효과성을 검증하기 위하여 침입탐지시스템에 제작된 열림/닫힘에 대한 탐지룰을 적용하여, 운전단말에서 열림/닫힘 명령 실행 시 침입탐지시스템에서 효과적으로 탐지 가능함을 실증하였다.

6.2.1 열림(Open) 제어명령 실행 탐지

운전단말에서 열림 제어명령 실행 결과, Table 4의 열림 탐지 공격명으로 탐지됨을 확인하였으며, 이를 통해 향후 시그니쳐 정밀화 연구를 통해 명령코드의 위·변조시 탐지 가능성을 확인하였다.

공격자	대상자	위험도	시도횟수	통신량	TTL	RAW	공격명
10.200.234.125	10.200.234.115:1027	보통	2	556B	128	✓	attack-scada-control(open).14101602@motiecsc
10.200.234.125	10.200.234.115:1027	보통	2	556B	128	✓	attack-scada-control(open).14101602@motiecsc
10.200.234.125	10.200.234.115:1027	보통	2	556B	128	✓	attack-scada-control(open).14101602@motiecsc
10.200.234.125	10.200.234.115:1027	보통	2	556B	128	✓	attack-scada-control(open).14101602@motiecsc
10.200.234.125	10.200.234.115:1027	보통	2	556B	128	✓	attack-scada-control(open).14101602@motiecsc

Fig. 20. Open-command detection in IDS

6.2.2 닫힘(Close) 제어명령 실행 탐지

닫힘 제어명령 실행 결과, Table 4의 닫힘 탐지 공격명으로 탐지됨을 확인하였으며, 이를 통해 향후 시그니쳐 정밀화 연구를 통해 명령코드의 위·변조시 탐지 가능성을 확인하였다.

공격자	대상자	위험도	시도횟수	통신량	TTL	RAW	공격명
10.200.234.125	10.200.234.115:1027	보통	2	556B	128	✓	attack-scada-control(close).14101601@motiecsc
10.200.234.125	10.200.234.115:1027	보통	2	556B	128	✓	attack-scada-control(close).14101601@motiecsc
10.200.234.125	10.200.234.115:1027	보통	2	556B	128	✓	attack-scada-control(close).14101601@motiecsc
10.200.234.125	10.200.234.115:1027	보통	2	556B	128	✓	attack-scada-control(close).14101601@motiecsc

Fig. 21. Close-command detection in IDS

6.2.3 ICMP Flooding 서비스거부공격 탐지

원격지 단말PC로 다량의 Ping을 이용한 서비스 거부공격 수행 시 침입탐지시스템에서 Ping 공격과 관련된 다수의 제조사 탐지룰로 정상 탐지됨을 확인하였다.

공격자	대상자	위험도	시도횟수	통신량	TTL	RAW	공격명
10.200.234.115	10.200.234.250:None	높음	148	228.22K	128	✓	ICMP Ping Of Death
10.200.234.115	10.200.234.250:None	높음	150	231.30K	128	✓	ICMP Ping Of Death
10.200.234.115	10.200.234.250:None	높음	154	237.47K	128	✓	ICMP Ping Of Death
10.200.234.115	10.200.234.200:None	높음	79	61.53K	128	✓	ICMP Tear Drop
10.200.234.115	10.200.234.200:None	높음	79	61.53K	128	✓	ICMP Tear Drop
10.200.234.250	10.200.234.115:None	높음	487	383.03K	128	✓	ICMP Tear Drop
10.200.234.115	10.200.234.250:None	높음	503	397.09K	128	✓	ICMP Tear Drop
10.200.234.115	10.200.234.250:None	높음	459	359.51K	128	✓	ICMP Tear Drop
10.200.234.115	10.200.234.250:None	높음	481	379.75K	128	✓	ICMP Tear Drop
10.200.234.115	10.200.234.250:None	높음	495	389.33K	128	✓	ICMP Tear Drop
10.200.234.115	10.200.234.200:None	높음	55	42.61K	128	✓	ICMP Tear Drop
10.200.234.250	10.200.234.115:None	높음	495	389.33K	128	✓	ICMP Tear Drop

Fig. 22. ICMP Flooding detection in IDS

6.2.4 UDP Flooding 서비스 거부공격 탐지

원격지 단말PC로 UDP Flooding 공격 툴을 이용하여 다량의 공격 수행 시 침입탐지시스템에서 UDP와 관련된 다수의 제조사 탐지룰로 정상 탐지됨을 확인하였다.

공격자	대상자	위험도	시도횟수	통신량	TTL	RAW	공격명
10.200.234.125	10.200.234.115:None	높음	22,821	33.42M	128	✓	UDP Tear Drop
10.200.234.125	10.200.234.115:None	높음	30,755	31.86M	128	✓	UDP Tear Drop
10.200.234.125	10.200.234.115:None	높음	14,411	14.92M	128	✓	UDP Tear Drop
10.200.234.125	10.200.234.115:6937	높음	2,322	3.59M	128	✓	UDP Flooding
10.200.234.125	10.200.234.115:56917	높음	1,090	1.69M	128	✓	UDP Flooding
10.200.234.125	10.200.234.115:0	보통	1,201	1.86M	128	✓	UDP Check Sum Error
10.200.234.125	10.200.234.115:0	보통	2,571	3.98M	128	✓	UDP Check Sum Error

Fig. 23. UDP Flooding detection in IDS

6.2.5 네트워크 웜·바이러스에 대한 차단

무작위 트래픽을 생성하여 확산시키는 네트워크 웜·바이러스와 유사한 특성을 패킷 발생기를 이용하여 재연하였다. 이후 시뮬레이션 환경과 무관한 IP

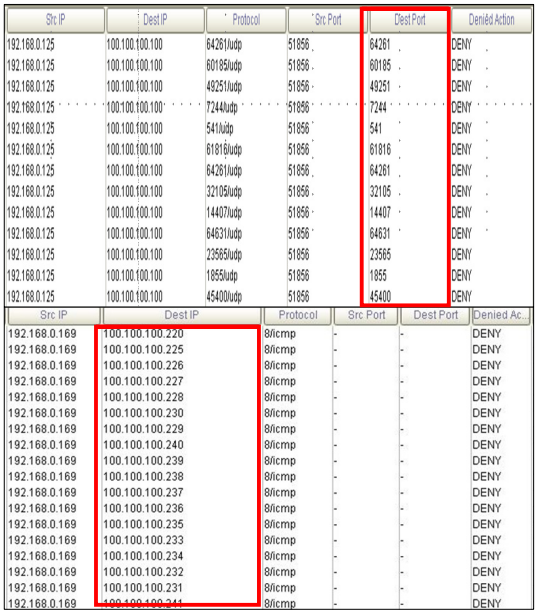

Fig. 24. Malicious traffic protection in Firewall

와 Port로 유해 트래픽 발생 시 원격지 네트워크로 확산되는 과정에서 네트워크 접점구간에 설치된 침입차단시스템에서 완벽히 차단되어 피해확산 방지가 가능함을 확인하였다.

본 연구에서 네트워크 보안관제 모델로 제시된 네트워크 구성과 유사한 시뮬레이션 환경을 구축하여 실증한 결과, 침입탐지시스템에서 다양한 서비스거부 공격 및 시그니쳐로 개발한 중요 제어명령에 대한 실행이나 위·변조에 대한 실시간 탐지가 가능함을 확인하였다. 또한, 네트워크 웜·바이러스와 같이 무작위 생성된 유해 트래픽의 원격지 확산 시 침입차단시스템에서 안정적으로 차단 가능함을 확인하였다.

결론적으로 본 논문에서 에너지 기반보호시설의 보안관제 방향성으로 제안한 네트워크 보안관제 모델이 zero-day 공격이나 정상 서비스를 이용한 APT 공격 등 unknown-attack에는 추가적인 분석 등 한계가 존재할 수 있지만, known-attack에 대해서는 완벽한 탐지가 가능함을 실증하였다.

VII. 결 론

외부와의 연계 접점구간을 안전한 자료연계방식의 하나인 물리적 일방향통신장치를 이용하여 외부의 침입가능성을 원천 차단하였다 하더라도, 성능분석이나 유지보수 등 자료 취득을 위해 노트북이나 USB 등 외부저장매체의 무분별한 사용으로 악성코드 감염사례가 종종 발생되고 있다. 지금까지의 제어시스템에 대한 보안관리정책은 주로 관리적·물리적인 접근 통제방법에 치중하여 운영되었으나, 본 연구에서는 제어시스템에 대한 보안관제 필요성을 역설하였으며 지능화되고 고도화되고 있는 제어시스템에 대한 사이버 공격으로부터 에너지 기반보호시설에 대한 안전성을 강화하기 위해서는 기존 관리적·물리적 접근통제의 한계를 인정하고, 제어시스템 내부 트래픽에 대한 능동적인 보안관제 필요성을 강조하였다. 무엇보다 지난 수년간 제어시스템 이상 징후 탐지 방법론에 대한 국내·외 수많은 논문이 발표되었지만 본 논문에서는 제어시스템에 대한 탐지 방법론 제시에 국한하지 않고, 제어시스템 내부 트래픽에 대한 적극적인 보안관제 수행을 위해서는 침입탐지시스템이나 침입차단시스템과 같은 보안시스템을 어떻게 배치해야 효과적으로 이상 징후 탐지가 가능한지 실제 현장에 적용 가능한 구체적인 네트워크 보안관제 모델과 방향성을 제시하였다는데 의미를 부여할 수 있다.

또한 본 연구에서는 zero-day 보안취약점 탐지 한계를 가지고 있는 시그니쳐기반 탐지방법을 새로운 시각에서 제어시스템의 가용성에 직접적인 영향을 미칠 수 있는 중요 제어명령을 분류하고, 이에 대한 실행이나 위·변조에 대한 이상 징후를 실시간 탐지 가능한 탐지패턴으로 제작할 수 있는 방향성을 제시하였으며 유사한 시뮬레이션 환경에서 효과적인 탐지가 가능함을 실증하였다는데 의미를 부여할 수 있다.

향후 연구방향으로는 중요 제어명령에 대한 실행이나 위·변조 상황의 실시간 탐지 정확도를 높이는 시그니쳐 정밀화 연구와 본 연구에서는 제어시스템 외부 연계접점 구간의 물리적 일방향통신장치 적용 등 보안조치로 제어시스템에 악성코드가 유입 될 수 있는 가능성을 USB 등 외부저장매체를 연결할 필요가 있는 컴퓨터단말로 국한하여, 제어용 컴퓨터단말에서 발생 가능한 이상 징후 탐지에 집중하였으나, 향후 IED (Intelligent Electronic Device)와 같은 TCP/IP기반의 현장 필드장치의 산업현장 확대에 대비한 연구가 필요하리라 판단된다.

References

[1] Dong-hwi Lee, Kyong-ho Choi, "A Study of an Anomalous Event Detection using White-List on Control Networks,"

Convergence security journal, 12(4), pp. 78-84, Sep. 2012.
〔2〕 Pauline Koh, Hwa-jae Choi, Se-ryoung Kim, Hyuk-min Kwon, Huy-kang Kim, "Intrusion Detection Methodology for SCADA system environment based on traffic self-similarity property," Journal of the Korean Institute of Information Security and Cryptology, 22(2), pp. 267-281, Apr. 2012.
〔3〕 K. Stouffer, J. Falco, and K. Kent, "Guide to supervisory control and data acquisition (SCADA) and industrial control systems security," Recommendations of the National Institute of Standards and Technology, pp. 498-506, Sep. 2006.
〔4〕 D. Yang, A. Usynin, and J. Hines, "Anomaly-based intrusion detection for SCADA systems," 5th International Topical Meeting on Nuclear Plant Instrumentation Controls and Human Machine Interface Technology, Nov. 2006.
〔5〕 R. Ramos, R. Barbosa, and A. Pras, "Intrusion detection in SCADA networks," Mechanisms for Autonomous Management of Networks and Services, LNCS 6155, pp. 163-166, 2010.
〔6〕 A. Carcano, I.N. Fovino, M. Masera, and Alberto Trombetta, "State-based network intrusion detection systems for SCADA protocols: a proof of concept," Critical Information Infrastructures Security, LNCS 6027, pp. 138-150, 2010.
〔7〕 Wan-jib Kim, Huy-kang Kim, Kyung-ho Lee, Heung-youll Youm, "Risk Analysis and Monitoring Model of Urban SCADA Network Infrastructure," Journal of the Korean Institute of Information Security and Cryptology, 21(6), pp. 67-81, Dec. 2011.
〔8〕 Homeland Security, ICS-CERT Year in Review, 2013
〔9〕 NCSC, MSIP, KCC, MOSPA, 2013 White Paper on National Intelligence, pp. 99-102, 2013
〔10〕 NCSC, The security guidelines for SCADA systems in national infrastructure, Apr. 2010
〔11〕 US Department of Commerce, NIST Special Publication 800-82, Guide to Industrial Control Systems(ICS) Security, June 2013

〈저자소개〉

장 정 우 (Jeong-woo Jang) 정회원
2015년 02월: 고려대학교 정보보호대학원 석사
2001년 3월~현재: 한전케이디엔(주) 근무
2008년 6월~현재: 산업통상자원 사이버안전센터 관제대응팀 과장
〈관심분야〉 정보보호, 네트워크 보안, SCADA 보안

김 우 석 (Woo-suk Kim) 정회원
2002년 8월: 광운대학교 정보과학기술대학원 석사
2013년~현재: 고려대학교 정보보호대학원 박사과정
2007년 12월~현재: 한전케이디엔(주) 근무
2008년 6월~현재: 산업통상자원 사이버안전센터 관제대응팀 과장
〈관심분야〉 정보보호, 디지털 포렌식, SCADA 보안

윤 지 원 (Ji-won Yoon) 종신회원
2003년 2월: 성균관대학교 정보공학사 졸업
2005년 2월: University of Edinburgh, 정보학과 석사 졸업
2008년 11월: University of Cambridge 전자공학과 박사 졸업
2008년 2월~2009년 5월: University of Oxford, 로봇연구소 박사후과정
2009년 5월~2011년 5월: University of Dublin 통계학과 연구원 및 강사
2011년 7월~2012년 8월: IBM 연구소 정규 연구원
2012년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 신호정보처리, 응용통계, 빅데이타 분석 기술, 도감청 탐지기술