情報保護學會論文誌
第 21 卷 第 6 號, 2011. 12

도시 기반시설 SCADA 망의 위험분석 및 모니터링 모델 연구

김 완 집,[1†] 김 휘 강,[2] 이 경 호,[2] 염 흥 열[1‡]
[1]순천향대학교, [2]고려대학교

Risk Analysis and Monitoring Model of Urban SCADA Network Infrastructure

Wanjib Kim,[1†] Huy Kang Kim,[2] Kyungho Lee,[2] Heung Youl Youm[1‡]
[1]Soonchunhyang University, [2]Korea University

요 약

최근 세계 각지에 국가 주요 산업시설을 목표로 하는 스턱스넷(stuxnet)과 같은 '사이버 무기'가 나타나 보안전문가들이 주목하고 있다. 도시의 교통과 지하철, 상수도 등과 같은 기반시설을 제어하는 네트워크는 전통적으로 폐쇄망으로 운영되고 있어 바이러스, 악성코드 등의 위협에 안전한 것으로 인식되어 왔으나, 이제는 새로운 공격 위협에 능동적으로 대처해야 할 때이다. 본 연구에서는 도시 기반시설 SCADA망의 제어시스템 현황과 위험을 분석하고, 운영환경에 맞는 보안 모델을 수립함으로써 이러한 위협에 대응하기 위한 방향을 제시하고자 한다.

ABSTRACT

In recently years, there are cyber-weapon aim to national infrastructure such as 'stuxnet'. Security experts of the world are paying attention to this phenomenon. The networks which controls traffic, subway, waterworks of the city are safe from threats such as computer virus, malware, because the networks were built on closed-networks. However, it's about time to develop countermeasure for the cyber-weapon. In this paper, we review status-quo of the control systems for metropolitan infrastructure and analyze the risk of industrial control system in SCADA(Supervisory Control And Data Acquisition) network. Finally, we propose a security model for control systems of metropolitan infrastructure.

Keywords: SCADA, Network Monitoring, stuxnet, Risk Management

I. 서 론

도시 기반시설을 제어하는 컴퓨터 시스템은 전통적으로 폐쇄망으로 운영되고 있어 일반적인 개방형 네트워크에서의 바이러스, 악성코드 등과 같은 외부 위협으로부터 안전한 것으로 인식되어 왔다. 그러나 최근 이란 부셰르 원전을 감염시켜 발전 설비의 오동작을 일으킨 스턱스넷(stuxnet)이라는 신종 악성코드가 등장하여 각국의 보안전문가들이 주목하고 있다.

기존의 악성코드가 자기과시나 금전적인 이득을 목적으로 한 것과 달리 스턱스넷은 보안위협의 패러다임을 바꾸는 차원이 다른 악성코드로서 '국가의 주요 산업시설 파괴 및 교란'을 목적으로 만들어졌다. 이로 인

† 주저자, kimwj@seoul.go.kr
‡ 교신저자, hyyoum@sch.ac.kr

해 스턱스넷은 악성코드가 사이버 무기화된 첫 번째 사례로 주목받고 있는 것이다.

인터넷망과 격리되어 운영되어 오던 기반시설 제어시스템도 이제는 원격 유지보수, 모바일 장치의 활용도 증대, USB를 통한 이동형 저장매체 사용 등과 맞물려 다양한 형태의 접근이 불가피한 환경에 놓이게 되었다. 이러한 환경의 변화는 결국 시설제어시스템도 폐쇄망이라는 특성으로부터 비롯된 안전성이 더 이상 유지되기 어렵다는 것을 뜻한다.

발전설비와 제어시스템 중에서도 특히 도시 기반시설을 제어하는 컴퓨터 시스템과 관련 네트워크는 파괴되거나 오동작을 일으킬 경우, 사회 전반에 막대한 혼란을 야기할 수 있기 때문에 더욱 철저한 보안 대책이 필요하다. 시스템을 운영 및 관리하고 있는 조직의 보안 인식이 제고되어야 하며, 정책과 절차에서부터 기술적인 보호조치, 사고 대응에 이르기까지 체계적인 관리체계가 수립되어야 한다.

그러나 도시 기반시설의 제어시스템은 무중단 운영과 상시적인 가용성이 최우선으로 확보되어야 하는 시스템이다. 따라서 시스템의 자체 보안 강화를 위하여 시스템의 보안패치, 악성코드 방지 소프트웨어의 설치 등과 같은 기술적인 조치를 취하는 것이 현실적으로 어렵다. 이와 같은 조치는 자칫 시스템의 가용성을 저해하거나 오류를 일으킬 수 있는 소지가 있기 때문에 충분한 검토와 시험의 선행이 요구된다.

아울러 시스템을 운영하는 조직의 특성을 반영한 보안 모델이 수립되어야 한다. 대부분의 제어시스템은 인위적인 조작이 아닌 자동제어를 기본 기능으로 하고 있다. 따라서 시스템 운영 조직의 구성원들은 대부분 반복적인 운영 업무에 숙련되어 있으며, 시스템의 장애 발생에 따른 기술적 대처 능력이나 분석 능력은 상대적으로 낮은 것이 현실이다. 이런 상황에서 조직의 역량을 강화하는 교육·훈련을 계획하는 것은 비효율적이며, 그 효과 또한 보장할 수 없다. 따라서 유관 기관이 참여하는 능동적인 지원체계가 고려되어야 한다.

본 연구에서는 OO시의 지하철, 교통, 상수도 기반시설 SCADA망과 관련 제어 컴퓨터를 대상으로 하여 보안 현황을 파악하고, 위험을 분석함으로써 SCADA 망의 외부 위협에 능동적으로 대처할 수 있는 종합적인 대응모델을 수립하고자 한다.

이를 위하여 기반시설 제어시스템 네트워크 구성상의 특징, 통신 프로토콜, 시스템 운영 환경을 면밀히 분석하고, 개선방안을 도출함은 물론, 네트워크상에서 이상징후를 사전에 탐지하기 위한 방법을 모색하고자 한다.

II. SCADA 네트워크 모니터링에 대한 문헌연구

SCADA 시스템 네트워크는 일반 네트워크와는 달리 열악한 환경에 강하며 네트워크 노이즈를 감당할 수 있는 장치들을 요구하고 있다.

초기의 SCADA 네트워크 상의 모니터링과 관련된 연구에서는 주로 이상증후 탐지(anomaly detection) 분야를 중심으로 진행되었다. 네트워크상에서 경량 모델과 퍼지 기법을 기반으로 진행한 이상 탐지 기법으로 가능성을 보였다.[6,7,8]

Cheung[6]의 연구에서는, Modbus TCP/IP 네트워크에서 동작하는 모델 기반의 침입 탐지 시스템을 제안하였다. 공개 침입탐지시스템인 Snort를 이용하였으며, Snort에서 룰셋을 직접 만들어서 사용하지는 않고, 플러그인 모듈을 추가로 작성하여 이벤트 교차 분석에 사용하였다. Sandia 국립 연구소에서 SCADA 테스트베드를 개발하여, 이 논문에서 제작된 툴을 이용, 통신패턴의 위반을 탐지한 결과 Modbus TCP/IP 네트워크에서 SCADA 네트워크를 효과적으로 모니터링할 수 있었다.

Verba[7]의 연구에서는, 트래픽의 상관관계에 기반하여 Man-in-the-Middle(MITM) 공격을 탐지하는 방법을 제안하였다. SCADA 네트워크에서 데이터와 명령어들의 흐름을 분석함으로써 공인되지 않은 명령 또는 장비간의 MITM 공격을 감지한다.

SCADA 시스템 내의 센서 네트워크에 침입 탐지의 연구도 진행되었다. P.Oman의 연구[9]에서는, 설정 정보 수집과 사용 명령어를 기록하고, 일일, 격주, 매월 측정한 자료를 검토하는 SCADA/센서 실험 환경 이벤트를 관제할 수 있도록 했다. 이를 위해 XML을 이용하여 IP, port, 사용 명령어 등의 SCADA 장비 정보를 기록하여 침입 패턴을 생성함으로써 침입을 탐지하고, RTU 설정 검색을 자동화 하는 시스템을 구현하였다.

SCADA 시스템 내에서 무선 센서 네트워크를 위한 IDS(Intrusion Detection System) 역시 모델 기반의 이상 탐지 기법에 초점을 맞춰 그 가능성을 보였다[10].

Holbert[8]의 연구에서는, 퍼지 하이브리드 시스템을 기반으로 전력 시스템의 상태 추정을 통한 모니터링 및 침입 탐지 방법을 제시하고, 가우스 소거법을 이용한 탐지의 오류 발생을 줄이는 방법을 제안하였다. 시뮬레이션 결과는 탐지 오류 없이, 낮은 비용으로 우수한 침입 탐지 성능을 나타내었다.

Tanya[10]의 연구에서는, WirelessHART 프로토콜 위에서 동작하는 모델 기반의 침입 탐지 시스템을 제안하였다. WirelessHART 프로토콜은 실제 산업 어플리케이션에서 쓰이는 강력하고 안정적인 개방형 무선통신 표준으로, SCADA 시스템에서 센서네트워크를 구축하기에 적합한 프로토콜이다. 이 연구에서 제안한 8 세트의 탐지 룰을 통해 물리계층, 데이터링크 계층, 네트워크 계층에서 신호 교란, 노드 손상, 패킷 변조, 패킷 재전송 등의 위협을 탐지한다.

Andrea[11]의 연구에서는, 정상적인 시스템의 작동을 방해하는 단일 Modbus 패킷 공격을 감지할 수 있는 상태기반 오용 탐지 침입 탐지 시스템을 제안하였다. 제안된 침입 탐지 시스템은 현재 상태의 분석을 통해 정상 패킷과 동일한 패킷임에도 악의적인 공격을 의미하는 패킷을 감지하는 것을 보여주었다.

관련 문헌을 분류하여 요약하면 다음 표와 같다.

〔표 1〕 SCADA 네트워크의 침입 탐지 시스템 종류

탐지 알고리즘	해당 연구	제안 방법	적용 프로토콜
이상 탐지 (anomaly detection)	[6]	Rule Modeling	Modbus TCP/IP
	[9]	Profile based	TCP/IP
	[10]	State Series Modeling	WirelessHART
오용 탐지 (misuse detection)	[7]	Signature Matching	
	[11]	Signature Matching	Modbus
hybrid	[8]	fuzzy self-learning	

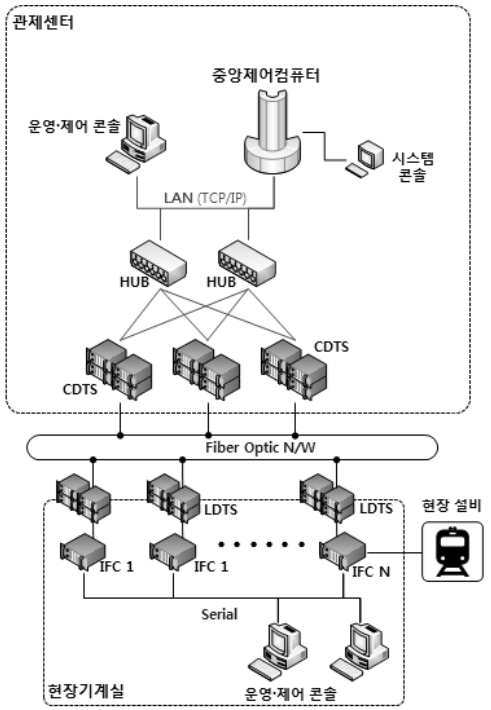
III. 도시 기반시설 SCADA 네트워크 보안

3.1 네트워크 구성

도시 기반시설을 제어하는 시스템은 대부분 폐쇄망으로 운영되고 있으며, 따라서 외부에서의 접근경로는 원천적으로 단절되어 있다. 또한 네트워크의 가용성 및 안전성 확보를 위하여 시스템 설비와 통신 선로는 모두 이중화 구성을 갖추고 있는 것이 일반적이다.

일반적인 지하철 운행신호 관제 및 제어 시스템의 네트워크 구성은 관제센터의 중앙 네트워크와 지하철 연동역과 신호분소 제어를 위한 현장 네트워크로 나뉜다. 모두 원격접속이나 무선접속은 원천적으로 불가능한 전용회선으로 구축되어 있으며, RS232C와 같은 Serial 네트워크로 구성되어 있는 경우가 대부분이나, 최근에는 시스템 확장성 및 호환성을 고려하여 Ethernet 케이블로 구축되는 경우도 적지 않다. 그러나 기본적으로는 시설을 직접 제어하는 현장 네트워크는 Serial 네트워크를 고수하고 있다.

이와 같은 네트워크의 폐쇄적 특성 상, 별도의 보안장비는 도입되어 있지 않은 경우가 대부분이다. 이것은 오히려 시스템의 가용성을 저해할 우려가 있기 때문이며, 외부로부터의 접점이 근본적으로 차단되어 있기 때문에 불필요한 조치이다. 그러나, 최근에는 중앙의 행정 인터넷망에서 단순 모니터링 및 의사결정 지원을 위한 데이터 조회 목적으로 중앙 네트워크로부터 내부 행정 인터넷망으로 데이터를 단방향 전송하는 경우가 늘고 있다.



- CDTS: Central Data Transmission System, 열차집중제어장치(Centralized Traffic Control; CTC)내 데이터전송시스템을 의미함
- LDTS:Local Data Transmission System, 철도신호처리 시스템 내에서 역정보전송장치를 의미함
- IFC:궤도회로장치 내 Interface Computer

〔그림 1〕 지하철 신호제어시스템의 네트워크 구성

3.2 통신 프로토콜

과거로부터 별다른 시스템 변경 없이 운영되고 있는 대다수의 제어시스템들은 시스템의 구축 초기에 개발된 전용 프로토콜을 사용하여 시스템간 통신이 이루어지고 있다. 이와 같은 프로토콜은 방식에 따라 분류하는 규정은 존재하지 않으나, 산업 전반에 사용되고 있는 SCADA망의 프로토콜을 분석하여 보면 크게 다음과 같은 3가지 종류가 있는 것을 알 수 있다.

- 폴링(Polling) 방식
- 브로드캐스팅(Broadcasting) 방식
- Exception Report 방식

폴링(Polling)방식의 프로토콜은 Master에서 데이터를 요구할 때만 Slave가 응답하는 구조를 가진다. Master가 적시에 필요한 데이터를 요청할 수 있어야 하기 때문에 이 방식의 도입을 위해서는 네트워크의 부하가 없어야 하며, Master의 최적화가 중요하다. 거의 대부분의 PLC(programmable logic controller)와 RTU(remote terminal unit, 원격단말장치)가 이 방식을 지원한다.

브로드캐스팅(Broadcasting) 방식은 Slave에서 무조건 데이터를 전송하는 구조이며, Master에서는 받은 데이터를 분석하기만 하면 된다. 이 방법은 많은 부하를 일으킬 수 있어 요즘은 아주 소량의 데이터를 주기적으로 전송하는 특수 컨트롤러 외에는 거의 사용을 하지 않는다.

Exception Report 방식은 Slave에서 변화가 있는 데이터만 통신하기 위하여, 변화가 있는 데이터에 대해서 이벤트를 발생시키며, Master에서는 이 데이터만을 읽는 구조로 되어 있다. 이 방식은 변화된 데이터만 통신하기 때문에 프로토콜 구조만 보면 가장 최적화된 통신 기법이라 할 수 있다. 대체로 DCS(distributed control system, 분산제어시스템) 및 여러 RTU 제품에서 많이 사용하고 있다.

3.3 운영·관리 환경

제어시스템은 자동화된 제어 기능을 중단 없이 안정적으로 수행하는 것을 일차적인 목적으로 하여 설계되어 있으며, 운영·관리의 목적 또한 시스템의 오류를 모니터링하고 안정성을 저해하는 요소를 차단하는 것을 기본으로 하고 있다. 통상의 제어시스템 운영·관리 환경에서 단계적 보안 조치는 크게 세 가지로 구분된다.

첫 번째로 우선시되는 안정성 저해요소의 차단 방법은 물리적인 접근통제이다. 시스템이 위치하고 있는 기계실이나 제어실, 관제실 등의 장소는 통제구역으로 설정되어 있으며, 출입통제를 위한 시건장치와 기초적인 외부인 출입 기록의 관리가 이루어진다.

둘째, 시스템 접근통제는 이러한 통제구역의 출입이 허용된 사람이 시스템의 이용을 위해 콘솔(console)과 같은 입출력 장치의 접근권한을 획득하기 위한 인증 장치로서, 시스템 계정 정보를 체계적으로 관리함으로써 구현된다. 일반적으로는 계정정보가 직무별로 구분되어 있거나 변경관리가 주기적으로 이루어지는 경우보다는 교대 근무의 특성 상, 업무효율을 위하여 단일 혹은 소수의 계정을 변경 없이 공유하여 사용하는 경우가 많다.

셋째, 보안 장비 혹은 보안 소프트웨어를 통한 기술적인 보호조치로서 권한을 획득한 사용자의 악의적인 행위를 탐지하거나 방어하는 단계이다. 그러나, 앞서 언급한 바와 같이 시스템의 가용성을 확보하는 것이 가장 우선시 되는 운영 목적인만큼, 이러한 활동은 현실적인 제약이 따른다. 특히 가동 중인 시스템은 MS-DOS, Windows NT 4.0, Windows 2000 등 벤더의 지원이 더 이상 이루어지지 않아 OS의 패치가 불가능한 구형 시스템이 많으며, 폐쇄망으로 구성되어 있어 네트워크를 통한 보안 소프트웨어의 업데이트도 용이하지 않다.

도시 기반시설 SCADA망과 제어 시스템들은 안정성을 최우선으로 하여 가동되고 있으며, 가용성 측면에서 보호되어야 할 자산들을 다수 포함하고 있다. 이러한 특성을 가진 시스템의 위협 시나리오를 정의하고, 이에 따라 시스템의 위험을 평가함으로써 조치 및 개선과제를 도출하되, 보다 현실적인 보안모델 수립을 위하여 운영·관리 환경의 특수성이 이해되고 반영되어야 한다.

IV. SCADA 네트워크에 대한 공격 위협

4.1 위협 주체 정의

도시 기반시설의 제어시스템에 대한 위협은 적대적 정부, 테러 집단, 산업 스파이, 불만 있는 직원, 악의적인 침입자와 같은 적대적 원인과 시스템 복잡성, 사람에 의한 오류와 사고, 장비 고장 및 자연 재해와 같

은 자연적인 원인과 같은 다양한 원인으로부터 생겨난다.

깊이 있는 방어 전략의 수립을 위해 적대적인 위협 주체를 NIST (National Institute of Standards and Technology)의 Special Publication 800-82 (이하 SP800-82)[1]에서는 다음과 같이 크게 10가지로 분류하여 정의하고 있다.

- 공격자 (Attacker)
- 봇넷 조작자 (Bot-network operators)
- 범죄 집단 (Criminal Groups)
- 대외 정보기관 (Foreign intelligence services)
- 내부자 (Insiders)
- 피싱 사기꾼 (Phishers)
- 스팸 발송자 (Spammers)
- 악성코드 제작자 (Spyware/malware authors)
- 테러리스트 (Terrorists)
- 산업스파이 (Industrial Spies)

기반시설 제어 네트워크에 대한 적대적인 외부 위협의 주체는 다양한 형태로 존재하고 있으며, 각 위협 주체는 그 침해 행위의 목적에 따라 분류된다.

그러나, 폐쇄적인 제어 네트워크 환경을 고려해볼 때, 전통적인 해커, 피싱(phishing) 사기꾼, 스팸 발송자 등과 같이 단순한 자기 과시나 금전적 이득을 취하기 위한 위협 주체나 불특정 다수를 대상으로 하는 위협 시나리오는 제외되어야 할 것이다.

기반시설을 공격하는 위협주체는 그 공격 대상이 명확하며, 해당 기반시설을 파괴함으로써 사회 혼란을 야기하거나, 시스템의 제어 권한을 악용하여 오동작을 일으킴으로써 정치적·반체제적 목적을 달성하려고 하는 경우가 대부분이다. 또한 테러를 목적으로 하는 경우에도 물리적인 공격이 아닌 시스템적 공격을 시도하기 위해서는 폐쇄망의 특성 상, 내부자를 통한 간접적인 접근이 유일한 방법이다.

결국, 물리적 접근이 용이하지 않고 외부망을 통한 네트워크 접근 경로가 차단되어 있는 시스템에 대한 위협 시나리오는 내부자를 통해 시스템에 간접 접근하여, 악성코드 등을 삽입하는 등의 오류를 발생시키는 행위를 취하는 방법이 될 것이다.

4.2 스턱스넷(stuxnet)의 동작 원리

이러한 위협 시나리오를 통한 다양한 공격 기법 중에서 최근 주목받고 있는 스턱스넷(stuxnet)의 동작 원리를 분석하여 그 대응방법을 연구해야 할 필요가 있다.

2010년 10월 행정안전부가 밝힌 자료에 따르면 세계 여러 나라에서 스턱스넷 공격에 따른 피해가 발생되는 것을 알 수 있다. 지금까지의 스턱스넷 피해 사례를 보면,

- 이란의 핵 시설에 스턱스넷 공격 (2010.1~2010.9)
  - 부셰르 원자력발전소 운영 시스템과 운영자 PC에 스턱스넷 침투
  - 나탄즈 우라늄 농축시설 스턱스넷 감염으로 수차례 오동작 유발
- 중국 내 주요 산업시설에 스턱스넷 공격 (2010.7)
  - 중국 600만 PC가 스턱스넷 감염, 주요 산업시설 공격
  - 중국의 철강, 전력, 원자력 등 주요 산업시설 스턱스넷 공격 피해
- 미국, 인도네시아, 인도, 파키스탄 스턱스넷 발견

등이 있다.

스턱스넷은 지금까지의 PC 바이러스와 다르게 단지 산업 핵심 시설의 파괴만을 목표로 하고 있다. 안철수 연구소 시큐리티 센터의 분석[2]에 따르면 스턱스넷은 여러 개의 파일로 구성되며, 산업자동화 제어시스템을 제어하는 PC에 Microsoft 운영체제 및 지멘스(Siemens)의 WinCC/Step7 관리도구가 설치되어 있을 경우 드롭퍼(Dropper)가 실행된다.

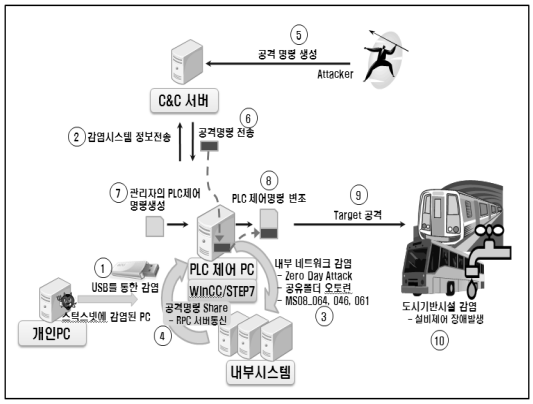
이 드롭퍼는 디렉토리 내에 있는 정상적인 s7otbxdx.dll 파일의 이름을 변경해 백업하고 정상 s7otbxdx.dll 파일과 동일한 이름으로 자신의 파일을 생성한다. 이후 산업자동화제어시스템을 통합 관리하는 도구인 Step7을 실행하면 원래의 정상파일이 아닌 스턱스넷이 실행된다. 이렇게 되면 감염된 산업자동화 제어시스템을 모니터링하거나 설비를 제어할 수 있게 되는 것이다.

〔그림 2〕의 스턱스넷 공격 과정을 보면,

① 스턱스넷에 감염된 PC에서 USB를 통해 PLC를 제어하는 메인 PC에 스턱스넷 전파

② 감염된 PC에서 C&C 서버로 감염 시스템 정보 전송

③ 악성코드 유포를 위해 내부 네트워크의 타 시스



〔그림 2〕 스턱스넷의 동작 흐름도

템 공격
④ 감염된 메인 PC와 추가 감염된 내부 시스템간의 공격 명령 공유
⑤ 악성코드 제작자의 공격 명령 생성
⑥ 공격 명령 전송
⑦ 관리자의 PLC 제어 명령 생성
⑧ PLC 제어 명령 변조
⑨ 타겟 공격
⑩ 설비제어 장애 발생

의 순으로 이루어진다.

스턱스넷은 공격목표가 PLC 제어명령 변조인 점과 대상시스템이 제어시스템이라는 점 등이 기존 악성코드와는 다른 패턴을 보여주고 있다. 하지만 유포 방식에 있어서는 USB라는 이동형 저장매체와 윈도우 OS의 취약점을 이용하고 있다. 그러므로 현장 엔지니어가 취할 수 있는 예방 방법은 USB 자동실행 방지, 최신 보안 패치 적용, 공유폴더 사용주의 등이 있다.

V. SCADA 네트워크에 대한 위험분석

5.1 위험분석 방법론

SCADA 네트워크 및 기반시설 제어시스템의 위험분석은 아직 그 방법론이 크게 발전되어 있지는 않다. 본 절에서는 전통적인 제어시스템의 위협주체와 위협시나리오, 취약점을 정의하고, 이를 토대로 하여 앞 절에서 연구한 도시 기반시설의 네트워크 구성 및 운영·관리 환경의 특성을 감안한 우려사항을 분석한다. 이를 위하여 미국의 NIST에서 발표한 SP800-82[1]을 근거로 하였다.

위험분석 방법론에 대해 ISO/IEC 27001[3]에서 제시하는 정보자산에 대한 위험분석 방법론을 바탕으로 미국 NIST의 SP800-82[1]의 이론을 접목하여 개념과 논리를 고찰하고자 한다.

위험은 자산의 가치와 위협의 발생빈도, 취약성의 정도를 합한 값이다.

$$\text{위험} = \text{자산} + \text{위협} + \text{취약성}$$
$$R_v = A_v + T_v + V_v$$

그런데, 여기에서 위협은 취약성을 이용하여 발생하는 경우가 대부분이며, 취약성과 연관성 없이 발생하기 어렵다. 따라서 특정 취약성과 위협은 하나의 조합으로 분석되어 나타낼 수 있으며, 본 연구에서는 이것을 '우려사항'으로 표현한다. 우려사항은 위협의 발생빈도와 취약성의 강도를 포함하고 있기 때문에, 하나의 우려사항 발생가능성 평가 값에 2를 곱하여 산출된다.

$$\text{우려사항} = \text{위협} + \text{취약성}$$
$$2 \times C_v = T_v + V_v$$

결국, 본 연구에서 사용하게 될 위험도 산출 공식은 다음과 같다.

$$\text{위험} = \text{자산} + \text{우려사항}$$
$$R_v = A_v + 2 \times C_v$$

정보자산 평가 기법은 정보자산 가치에 대한 BIA (Business Impact Assessment) 기법을 사용하여 정량화 하는 방법을 사용하였다.

개괄적인 위험 분석 절차는 아래와 같다.

- 1 단계 : 정보자산의 가치측정
- 2 단계 : 정보자산에 대한 위협요소 도출
- 3 단계 : 정보시스템의 취약성 파악 및 우려사항 정의
- 4 단계 : 위험도 산출
- 5 단계 : 보장수준 (Degree of Assurance) 평가

각 단계는 ISO/IEC 27001 에서 제시하는 위험분석 절차를 준수한다.

5.2 정보자산의 가치 측정

정보자산의 안전성은 3가지 측면에서 보장되어야

〔표 2〕 자산가치 평가 기준표

정보자산의 속성			평가 기준 (해당 속성이 결여되었을 경우의 영향도)
기밀성	무결성	가용성	
3	3	3	조직의 업무/기능이 중단될 정도로 치명적 손실 발생
2	2	2	조직의 업무/기능에 손실이 있으나 복구 가능
1	1	1	조직의 업무/기능에 무시될 정도의 영향만 미침
0	0	0	조직의 업무/기능에 영향이 거의 없음

한다. 기밀성(Confidentiality)은 해당 정보를 볼 수 있도록 허가받은 자만이 정보를 볼 수 있음을 보장하는 것이다. 무결성(Integrity)은 해당 정보가 원래 의도한 정보와 틀림없을 것을 보장하는 것이다. 가용성(Availability)은 해당 정보를 원하는 시간에 항상 사용할 수 있음을 보장하는 것이다.

정보자산의 가치는 해당 정보의 기밀성, 무결성, 가용성이 결여되었을 경우 발생하는 Impact(영향도)로 정의한다. 이에 대한 평가는 해당 자산의 소유자만이 가능하며, 평가를 위하여 사전에 등급(Scale)과 각 등급의 판단기준을 명시하고, 평가 결과는 유효성(Effectiveness)을 확보하기 위하여 현실과의 일치성을 검토한다.

평가 대상이 되는 정보자산은 그 범위를 기반시설을 직접 제어하는 시스템과 해당 시스템이 포함된 구간별 네트워크 등으로 정의하였다.

5.3 정보자산에 대한 위협요소 도출

앞 절에서 논의된 바와 같이 폐쇄 네트워크 환경에서의 위협은 대부분 내부자를 통한 경로로 유입된다. 내부자는 대상 시스템에 대해 잘 알고 있으며, 제한 없이 시스템에 접근할 수 있기 때문에, 시스템에 피해를 입히거나 시스템 데이터를 탈취하는 데에 큰 어려움이 없다.

외부 인력이 실수로 악성코드를 내부에 반입하는 것 또한 내부자 위협이라고 할 수 있다. 내부직원, 계약직원, 비즈니스 파트너들도 내부자의 범위에 둘 수 있다. 스턱스넷과 같은 악성코드가 이와 같은 경로로 내부 망에 유입되었을 경우, 정상적인 패킷으로 인식되기 때문에 사전에 탐지 및 분석하여 기술적으로 대응하기 어렵다.

부적절한 정책, 절차 및 테스트도 기반시설 제어시스템에 영향을 미칠 수 있다. 제어시스템과 외부장치가 받을 수 있는 영향은 사소한 피해부터 심각한 피해까지 다양하다. 내부자에 의한 의도되지 않은 영향은 가장 높은 확률로 발생한다.

5.4 정보시스템의 취약성 도출 및 우려사항 정의

외부로부터의 공격 위협들은 전형적인 설비제어시스템에서 발견되는 취약점을 이용하여 공격을 수행한다. 취약점들은 정책과 절차, 플랫폼 및 네트워크로 분류되어 있으며, 기반시설 제어시스템들은 대개 이러한 취약점의 범위를 크게 벗어나지 않는다.

이러한 취약성 중에서 본 연구의 평가 대상인 OO시의 지하철, 교통, 상수도 기반시설 SCADA망과 관련 제어시스템의 분석을 통하여 현실적인 위협과 조합이 가능한 취약성을 식별하여 도출하였다.

도출된 평가 대상 시스템의 취약성을 이용할 수 있는 위협 시나리오를 조합하여, 최종적으로 본 연구의 평가 대상인 OO시의 지하철, 교통, 상수도 기반시설 SCADA망과 관련 제어시스템의 '우려사항'을 정의하면 다음과 같다.

- 플랫폼 설정
  - 시스템 구축 시에 세팅된 디폴트 환경설정(불필요한 포트나 악용될 수 있는 구동 상태의 서비스가 활성화된)의 사용으로 내부자에 의한 공격 가능
  - 중요 환경설정이 백업되어 있지 않아 시스템 장애나 보안사고 발생 시 복구 어려움
  - 패스워드의 강도, 유지방법이 정의된 정책이 없

〔표 3〕 영역별 취약성 분포 (괄호 안은 개수)

구분	정책과 절차	플랫폼	네트워크
NIST의 SP800-82	· 정책과 절차(9)	· 설정(11) · 하드웨어(10) · 소프트웨어 (13) · 악성코드 방지 (3)	· 구성(6) · 하드웨어(5) · 경계(4) · 모니터링/로깅(2) · 통신(4) · 무선 연결(2)
평가 대상 시스템		· 설정(5) · 하드웨어(3) · 소프트웨어(6)	· 구성(2) · 경계(3) · 통신(2) · 무선연결(2)

거나 부족하여 시스템에 대한 패스워드의 노출 및 탈취 위험 있음
- 패스워드가 공유되거나 노출되는 경우 내부자에 의한 무단 액세스 가능
- 사람이나 컴퓨터 알고리즘에 의하여 추측 될 수 있는 패스워드를 사용하여 경우 무단 액세스 가능

• 플랫폼 하드웨어
- USB나 PS/2 포트가 물리적으로 차단되어 있지 않아 내부자가 이동식 저장매체, 키로거 등으로 접근할 수 있으며, 이로 인해 악성코드 유포 가능
- 장비/시스템에 대해 접근한 인원을 식별할 수 있는 내부자 접근기록과 같은 통제가 이루어지지 않아 시스템 장애나 보안사고 발생 시 책임 추적 어려움
- 장치에 2기 이상의 NIC가 탑재되어 있어 서로 다른 네트워크 구간 간에 인가되지 않은 데이터가 통과될 경우 시스템 장애, 보안사고 발생 가능

• 플랫폼 소프트웨어
- 해당 시스템에서 쓰이는 오래된 버전의 하드웨어, OS 및 애플리케이션에 서비스거부공격이 악용될 수 있어 내부자에 의한 시스템 장애, 보안사고 발생 가능
- 해당 시스템이 올바르지 않은 형태이거나 예기치 않은 필드 값을 포함하는 패킷에 취약하여 내부자에 의한 시스템 장애 발생 가능
- IDS, IPS(Intrusion Prevention System)의 부재로 웜에 감염되어 공격당한 내부 호스트를 식별하거나, DoS(Denial of Service) 공격을 중지/방지할 수 없음
- 패스워드가 정기적으로 변경되지 않아, 노출된 패스워드가 장기간 악용될 수 있음
- 해당 시스템에서 쓰이지 않으나 OS상에 활성화되어 있는 서비스들의 취약점으로 인해 내부자에 의한 시스템 장애, 보안사고 발생 가능
- 보안사고에 대비하여 시스템/애플리케이션/네트워크 관련 로그가 기록/검토되지 않아 사고 발생 시 책임추적이 어려움

• 네트워크 구성
- ACL(Access Control List)과 같은 데이터흐름제어에 의해 시스템의 직접적인 액세스가 제한되어 있지 않아 내부자에 의한 시스템 장애, 보안사고 발생 가능
- 부적절한 방화벽 설정과 라우터의 ACL에 의해 불필요한 트래픽이 유입될 수 있으며 이를 악용하는 내부자에 의한 시스템 장애, 보안사고 발생 가능

• 네트워크 경계
- 네트워크 경계 보안에 대한 정의가 되어 있지 않거나 명확하지 않아 시스템과 데이터에 대한 무단 액세스 가능
- 방화벽이 존재하지 않거나 구성이 부적절하게 되어 있어 서로 다른 네트워크간의 불필요한 데이터가 전달 될 수 있고, 이로 인해 시스템 장애, 보안사고 발생 가능
- 행정 네트워크와 해당 시스템 네트워크가 연계되어 있어 해당 시스템 네트워크에서 필요한 네트워크 트래픽 자원을 행정 네트워크에서 소모하여 해당 시스템의 가용성 저해 가능

• 통신
- 사용되는 프로토콜이 잘 알려진 프로토콜일 경우 내부자에 의해 해당 프로토콜의 취약점이 악용되어 시스템 장애, 보안사고 발생 가능
- 해당 시스템의 프로토콜에서 무결성검사가 이루어지지 않아 내부자에 의해 해당 시스템 데이터의 무결성을 보장받을 수 없음

• 무선 연결
- 무선 클라이언트와 AP(Access Point)간 적절한 상호인증절차가 없어 악의적인 내부자가 해당 시스템에 무단으로 액세스 가능
- 무선 클라이언트와 AP간의 민감한 데이터가 암호화되지 않아 악의적인 내부자에 의해 데이터가 노출되거나 변조될 수 있음

이와 같이 정의된 우려사항은 자산의 중요도 평가 결과와 함께 위험도 산정을 위한 중요한 지표의 하나로서 적용된다.

5.5 위험도 산출

정보의 영향도와 위협의 빈도, 취약성의 정도를 평가하여 위험도를 산출한다. 위험도는 위험이 높은 것

〔표 4〕 위험도 '상'의 비율 (단위: %)

대상 기반시설	지하철		상수도	교통
	M 社	S 社		
기밀성	60	57	73	71
무결성	61	65	55	63
가용성	48	49	46	48

부터 순서대로 나열되어 정리된다. 위험도가 가장 높은 것부터 각각 평가하여 조치를 취할 대상인지를 판단한다. 더 이상 조치를 취할 대상 위험이 아닌 감내할 만한 위험(Acceptable Risk)이라고 판단되면 그 정도를 DOA(Degree of Assurance)로 정의한다.

단, 앞 절에서 우려사항을 도출하는 과정에서 위험분석 대상이 되는 시스템과 네트워크의 특성에 따라 발생가능성이 현저히 낮은 위협과 취약점을 식별하여 제외하는 과정을 거쳤기 때문에 보장수준 평가를 위한 임계치(DOA) 설정은 무의미하다. 즉, 기 도출된 우려사항으로 평가되는 위험은 모두 '관리되어야 할 위험(Unacceptable Risk)'으로 판단하는 것으로 한다.

각 자산 속성별로 위험도를 상·중·하로 나누어 대상 기반시설의 종합 위험도를 산출한 결과, 위험도가 '상'인 비율은 아래 〔표 4〕와 같이 나타났다. 기존 시스템과 네트워크의 가용성 확보 중심의 설계와 구성으로 인하여 가용성 측면의 위험은 상대적으로 낮게 나타났다.

위험도 '상'은 위협의 빈도가 높고, 널리 알려진 취약성이 존재하여 그 발생가능성이 매우 높은 위험으로서 시급히 조치되어야 함을 의미한다. 즉, 해당 위험을 제거하는 조치를 취함으로써 위험의 상당 부분이 제거될 것이다.

상위 위험의 내용은 각 평가 대상 기반시설에 매우 비슷한 내용으로 나타났다. 위험도가 높게 산출된 정보자산에 해당하는 우려사항을 유형별로 분류하여 살펴보면 다음과 같다.

- 계정 및 패스워드 보안 정책 필요
  - 패스워드의 강도, 유지방법이 정의된 정책이 없거나 부족하여 시스템에 대한 패스워드의 노출 및 탈취 위험 있음
  - 패스워드가 정기적으로 변경되지 않아, 노출된 패스워드가 장기간 악용될 수 있음

- 물리적 접근 통제
  - USB나 PS/2 포트가 물리적으로 차단되어 있지 않아 이동식 저장매체, 키로거 등으로 악성코드 유입 가능
  - 장비/시스템에 대해 접근한 인원을 식별할 수 있는 내부자 접근기록과 같은 통제가 이루어지지 않아 시스템 장애나 보안사고 발생 시 추적 어려움

- 소프트웨어 및 네트워크 감시 강화
  - 해당 시스템에서 쓰이는 오래된 버전의 하드웨어, OS 및 애플리케이션에 서비스거부공격이 악용될 수 있어 내부자에 의한 시스템 장애, 보안사고 발생 가능
  - 해당 시스템이 올바르지 않은 형태이거나 예기치 않은 필드 값을 포함하는 패킷에 취약하여 내부자에 의한 시스템 장애 발생 가능
  - IDS, IPS의 부재로 웜에 감염되어 공격당한 내부 호스트를 식별하거나, DoS 공격을 중지/방지할 수 없음
  - 네트워크 경계 보안에 대한 정의가 되어 있지 않거나 명확하지 않아 시스템과 데이터에 대한 무단 액세스 가능

5.6 위험조치 범위 및 계획

위험조치 계획은 우려사항을 제거하기 위한 구체적인 개선방안이다. 단순한 시스템 설정 변경이나 조직의 시스템 운영 정책을 보완함으로써 조치할 수 있는 우려사항은 즉각적으로 제거하도록 하며, 이러한 활동들은 위험조치의 일차적인 범위로서 그 의미를 가진다.

그러나, 기반시설의 제반 설비를 운영하기 위한 SCADA 및 설비제어시스템은 전통적으로 안전성을 유지하기 위하여 폐쇄적인 네트워크로 구성되어 있으며, 한번 설치되면 가동을 중단하기 곤란한 특성 때문에 유지보수 과정에서의 시스템 업그레이드마저 쉽지 않은 환경에서 운영되어 오고 있다. 이러한 환경으로 인하여 매 시간 출현하는 사이버 공격의 새로운 위협에도 불구하고 악성코드에 대비한 운영 소프트웨어의 패치가 거의 이루어 지지 않고 있으며, 단순한 비밀번호의 변경에서부터 새로운 보안 소프트웨어 설치까지 보안성을 높이기 위한 추가적인 통제 적용이 곤란한 조건을 가지고 있다.

따라서, 스턱스넷을 포함한 새로운 보안 위협을 통

제하기 위한 대응책은 아래와 같은 조건을 전제로 설계되고 적용될 수밖에 없다.

- 기존에 설치된 시스템 및 소프트웨어를 변경하지 않는다.
- 시스템의 하드웨어와 소프트웨어 상에 보안 통제를 신규 또는 추가하여 적용할 수 없다.
- 시스템이 설치된 네트워크 트래픽을 직접 차단하거나, 변경하는 통제를 적용할 수 없다.
- 보안 통제를 적용하기 위하여 시스템을 다운시키거나 특정 소프트웨어를 재가동할 수 없다.
- 시스템이 존재하는 네트워크에 추가적인 네트워크 트래픽을 유발할 수 없다.

이러한 보안통제 환경의 제약으로 인하여 전통적으로 악성코드를 차단하기 위하여 활용되어 온 바이러스 백신, PC 보안 소프트웨어 및 PC 기반 NAC (Network Access Control) 등이 적용될 수 없는 환경이며, 네트워크 트래픽을 능동적으로 수집하여 검증하는 Gateway 방식의 보안통제도 운영하기 곤란한 특징이 있다.

본 연구에서는 이러한 SCADA 시스템의 특징적인 운영환경을 수용하면서 효과적으로 외부의 사이버 위협을 모니터링 및 차단하기 위하여,

- 기존 시스템 내부에 별도의 agent 프로그램의 설치 없이,
- 기존 네트워크 트래픽에 영향을 주지 않는 Passive 한 형태로 네트워크 트래픽을 수집하고,
- 스턱스넷 등 외부위협이 발생할 경우 나타나는 특징적인 네트워크 행태를 분석하며,
- 지속적으로 모니터링 하도록 Rule-set을 적용 및 운영할 수 있는 기반을 제공할 수 있는,
- 알려지지 않은 공격에 대한 대응이 가능한 형태의 모델 적용이 요구되므로

이러한 요구사항을 반영한 보안통제 모델을 수립하고 이를 검증하는 것을 목표로 한다.

VI. SCADA 네트워크 보안 모델 수립

SCADA 네트워크의 외부 위협에 대한 방어 전략은 위험조치계획 중에서 가용성을 침해할 위험이 있는 조치사항을 대체할 수 있는 대응 모델을 마련하고, 앞 절에서 논의된 바와 같이 운영 환경의 특수성에 기인한 제약사항에 위배되지 않는 보안모델을 수립하는 데에 그 핵심이 있다.

시스템의 안정적인 무중단 운영을 보장하기 위해서는 단순히 OS의 보안 패치, 보안 소프트웨어의 도입 및 설치, 보안 장비의 도입 등을 통해서 해결될 수 없다. 이러한 조치들은 또 다른 가용성 침해의 우려를 내포하고 있고, 이러한 능동적이고 기술적인 조치를 유지하고 관리하는 데에 많은 인력과 비용이 소요될 수밖에 없다. 따라서 SCADA 네트워크상의 패킷(Packet)을 Passive 방식으로 수집하여 모니터링하고, 이를 공동 대응하는 방법을 통해서 효과적인 보안 모델을 수립하고자 한다.

6.1 위협 탐지 모델

이상 징후를 탐지하는 방법론은 크게 두 가지 형태로 분류될 수 있다. 첫째, 네트워크 기반의 이상증후 탐지로서 정상적 특성 집단을 벗어나는 비정상 트래픽을 감시함으로서 탐지하는 기법이며, 둘째로 호스트 기반의 Signature based detection (시그니처 기반 탐지, misuse detection)으로서 시스템과 응용 프로그램의 알려진 취약점을 이용한 공격을 탐지하는 기법이다.

그러나, 본 연구에서 위험분석의 대상 시스템들은 대부분 알려진 취약점이 없는 모델이며, 스턱스넷과 같은 악성코드를 이용한 신종 공격은 알려지지 않은 공격 기법 들이다. 즉, Signature based detection 기법으로는 이러한 위협에 대비하기 어렵다.

보다 효과적인 이상 징후 탐지를 위해서는 네트워크 트래픽을 조사하고, 이를 분석하여 통계에 기반을 둔 비정상적 네트워크 트래픽을 판별하여 탐지하는 방법이 보다 발전적인 형태로 연구되고 있다.

SCADA 네트워크의 패킷 분석을 위하여 다음과 같이 두 가지 방법론[4][5]을 활용한다. 기존 [4][5] 연구에서 제시한 RFM(Recency, Frequency, Monetary) 기반 분석기법과 SPC(Statistical Process Control)의 경우, 네트워크 트래픽상의 특징값(feature)들을 선정하여 각 값들의 변화를 손쉽게 이해할 수 있으며, 기 제어시스템을 모니터링하는 인원들에게 친숙한 형태의 차트를 제공해 줄 수 있다는 점에서 네트워크 트래픽 기반 패턴 변화를 감지하기에 적절하다고 판단하였다.

6.1.1 RFM 분석기법

RFM 분석기법이란 주로 고객 행태 분석을 할 때

사용하는 방법이며, 특정 객체의 행동을 분석할 때 R (Recency), F (Frequency), M (Monetary) 의 의미에 부합하는 변수를 특징값으로 이용하여 패턴을 모델링하고 분석하는데 적합한 방법이다[13].

이 RFM 분석기법을 보안에 응용하여 트래픽이나 시스템 행태에 대해 다음과 같이 변수 모델링을 할 수 있다.

R값은 보안과 관련된 이벤트가 가장 최근에 언제 일어났는가를 의미하며, F 값은 보안과 관련된 이벤트가 어떤 주기로 어떤 빈도로 일어났는가를 의미한다. 즉 최근에 일어나고 있는 보안에 관련된 이벤트일수록 주의를 기울여 진단해야 하며 주기적으로 잦게 일어나는 보안에 관련된 이벤트나 주기가 점점 짧아진다든가 사건발생을 암시하는 쪽으로 변화하고 있다면 이 역시 주의를 기울여 진단해야 한다. 또 M 값은 이벤트 발생 총량으로써, 네트워크 프로토콜별 패킷 총량은 얼마인가, 포트 별 패킷 사이즈 총량은 얼마인가 등의 정량적인 척도로 사용되게 된다.

이 RFM 값을 이용하여 분석하기 쉽도록, 입력 데이터로 네트워크 프로토콜의 분포, 프로토콜별 목적지 포트 분석, 패킷 사이즈 분석을 통하여 각 시스템과 네트워크의 Profile을 만들게 된다.

어떤 변수가 정상분포를 따르면서 변동의 폭이 크게 발생할 확률이 높지 않다면, 통계적 기법을 이용하여 이상증후를 탐지하기에 훨씬 용이한데, SCADA 제어망의 경우 폐쇄망에서 규칙적인 작업 위주로 트래픽이 발생하기 때문에 이런 통계적 기법에 의한 Profiling 은 더욱 효과적으로 적용될 수 있다.

6.1.2 통계적 공정관리(SPC) 기법

RFM 분석 기법과 병행하여 이상증후를 손쉽게 감지할 수 있도록 데이터의 용이한 시각화를 위해 통계적 공정관리(SPC, Statistical Process Control)에서 사용하는 관리도 (Control Chart)를 이용한다.

통계적 공정 관리란, 의도하는 품질의 제품이 생산될 수 있도록 공정을 관리, 감독하는데 쓰이는 통계기반 응용 방법으로 정의할 수 있다. SPC는 수집된 데이터는 표준 정규 분포를 띄고 있으며, 모든 공정은 변동 사항이 발생 가능하다는 가정 하에서 사용된다. 특히 통계의 변동이 이상 원인에 의하여 발생했을 때 이를 즉각 알려주어 조치를 취할 수 있게 해줄 수 있는 기능이 특징적이라 할 수 있다.

일반적으로 정상적으로 운영되는 네트워크의 경우, 특히 제어망과 같이 동일한 네트워크 트래픽이 주기성을 가지고 발생하는 특징을 가진 경우에는, 통계적 공정관리기법을 네트워크 트래픽 이상 징후 탐지기법에 적용할 수 있으며 관리도 (Control Chart) 를 사용하여 분석을 할 때, 관심 있는 임의의 통계량 (표본평균, 표본표준편차, 표본범위 등)이나 임의의 품질특성치의 평균을 나타내는 중심선(Center Line)과 중심선 상하에 한 쌍의 관리한계선(Control Limits)으로 구성된 그래프를 이용하며, 이것을 사용하는 방법을 관리도법 (Control Charts Method)이라고 칭한다.

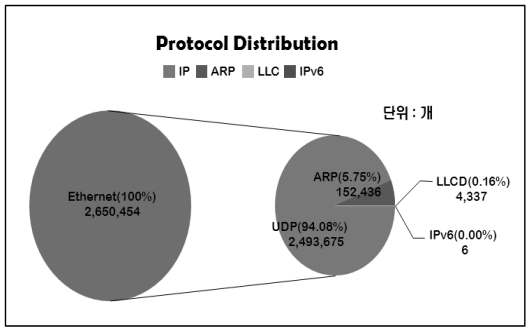
모든 시스템의 행동패턴 중에서 네트워크 프로토콜의 분포, 프로토콜별 목적지 포트, 프로토콜별, 포트별 패킷 사이즈 등이 일반적으로 정규분포를 따른다고 가정하여 시스템의 관찰된 변동 상황이 정상인지 비정상적인지를 관리도(control chart)를 이용하여 파악한다. 이벤트의 평균값을 구한 뒤, 정규분포를 따르는 이벤트라면, 시스템의 행동패턴은 $\mu \pm 2\sigma$ (이때 μ는 평균, σ는 표준편차)의 범위내에 99.73%의 이벤트가 분포하게 된다. 이를 기준으로 삼아서 관리상한(upper control limit)을 $\mu + 2\sigma$로, 관리하한(lower control limit)을 $\mu - 2\sigma$ 로 잡은 뒤, 이 영역을 벗어난 경우 이상증후를 가지고 있다고 판단할 수 있다.[12]

관리 상한과 하한을 벗어나는 데이터에 대한 이상원인 진단 외에도 공격자가 장기적으로 자신의 패턴변동을 조금씩 주면서 점진적인 변화를 주는 경우에 대비하여 시스템의 패턴이 연속 3회 이상 한 방향으로 증가하는 추세를 보이고 있지 않는가에 대한 이상진단도 수행한다.

6.1.3 패킷 데이터 분석 결과

본 논문에서 제안한 네트워크 보안모델의 유효성을 검증하기 위해, OO시 도시기반시설의 네트워크 패킷 데이터를 수집하여 분석에 적용하였다. 지하철과 상수도 부문의 시설 제어 네트워크의 패킷 데이터를 Passive하게 수집하였고, 수집한 데이터를 기반으로 RFM특성치에 따른 프로파일링을 하였으며, 이 데이터에 관리상한과 하한을 관찰하여 이상증후 감지가 가능하겠는가를 중심으로 분석하였다.

네트워크 트래픽은 serial 통신 구간을 지나 관제 및 통제장비의 바로 앞단의 스위치에서 트래픽을 스위치에서 포트 미러링하여 덤프하였으며, 모두 Ethernet emulation 이 되어 있고 TCP/IP 트래픽의 형



〔그림 3〕 프로토콜 분석 결과 (상수도 부문)

태로 구성되어 있다. 제어용 트래픽의 특성상 폴링 방식으로 주기성을 뚜렷이 갖는 특징이 있다. 대부분의 제어명령들이 UDP로 전송되는데, 제어용 트래픽의 프로토콜 별 분포는 아래 그림에서와 같이 UDP, ARP, LLC, IPv6의 순으로 나타났다.

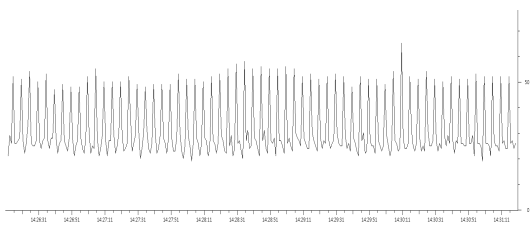
정수 시설의 네트워크 패킷은 시스템이 장기간 변함없이 주기성을 가지고 운영되는 제어망의 특성상 특성치 값이 변화를 거의 보이지 않는 패턴으로 나타나고 있다. 이것은 지하철 기반시설의 SCADA망과 신호 제어시스템에서도 유사하게 나타났다.

전력망의 경우에는 LLC가 85.6%, UDP가 14%, 기타 IP트래픽이 14%로 분포하나 주요 제어 트래픽이 UDP를 통하여 주기성을 가지고 발생한다는 점에서는 동일하다.

전체 트래픽을 분석하여 1초 단위 시간의 흐름에 따라 표현하면 〔그림 4〕과 같이 나타난다.

X축은 시간의 흐름을 나타내며, Y축은 1초당 패킷 수를 나타낸다. 상기 데이터는 하루 동안의 데이터이며, 위와 같이 계속적으로 동일한 패턴의 주기를 이루는 모습이 관찰되었다. 전반적으로 F(Frequency) 값의 주기값과 각 빈도별 패킷량인 M(Monetary) 값 역시 정상적인 시스템 운영의 범주에 수용된다고 보여진다.

결론적으로 네트워크 패킷 데이터 자체에 뚜렷한 패턴이 존재하기 때문에 RFM 값을 기준으로 한 SPC 기법과 이를 시각화 한 관리도를 통해 이상증후 측정이 가능하다.



〔그림 4〕 트래픽 분석 결과 (상수도 부문)

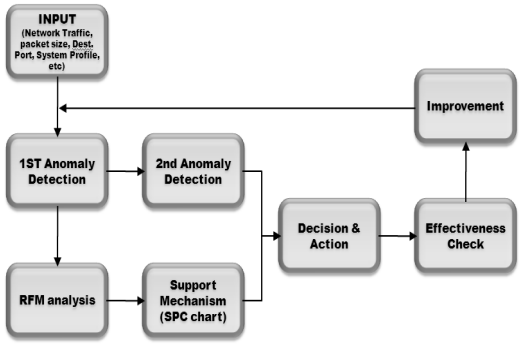
6.2 위협 분석 및 대응 모델

본 연구에서는 일반적인 SCADA 환경에서 적용할 수 있는 이상 징후 탐지모델을 수립하기 위하여 실제 SCADA 환경과 동일한 조건에서 운영되는 시뮬레이터의 네트워크 트래픽을 수집하여 RFM 분석 및 SPC 차트를 활용한 분석을 통하여 고찰함으로서, SCADA 환경에서의 침입탐지 및 대응에 대한 의사결정이 가능한 분석 및 대응 모델을 〔그림 5〕와 같이 도출하였다.

이 분석체계의 입력으로는 네트워크 프로토콜의 분포, 프로토콜별 목적지 포트, 포트 별 패킷 사이즈 등과 기존에 구축된 시스템 프로파일이 활용 되며, 1단계 및 2단계로 이상증후 탐지를 하는 과정에서 RFM 분석 및 SPC 차트를 활용한 분석이 이루어져 출력으로서 최종 판단을 도출하게 된다.

이러한 결과 값은 실행에 옮겨진 후 그 유효성을 검증하는 절차를 통하여 개선할 사항을 도출하여 피드백 함으로서 1단계 및 2단계의 이상증후 탐지의 False Positive 및 False Negative 를 최소화 할 수 있다.

기존의 침입차단시스템이 시스템에 직접 설치되고, 정의되어 있는 Rule에 기초하여 작동하기 때문에 오랜 기간 동안 조금씩 이루어지는 공격에 대한 탐지 및 변종 탐지가 곤란한데 반하여, 이 모델은 네트워크에서 Passive 하게 설치되어 네트워크 트래픽을 수집함으로서 기존에 설치된 시스템과 네트워크에 전혀 영향을 끼치지 않고, 네트워크의 행위에 기반을 두어 트



〔그림 5〕 분석 및 대응 프로세스 다이어그램

래픽을 분석함으로써 구축된지 오래되어 기존 시스템 내부에 새로운 보안 모듈의 설치가 불가능한 SCADA 환경에서도 침입을 탐지할 수 있게 된다. 한걸음 나아가 장기간에 걸쳐서 점진적으로 이루어지는 공격에 대해서도 일정 횟수의 동일 방향에 대한 행위 수집 룰을 부여함으로서 탐지가 가능하게 되었다.

다만, 본 연구 역시 네트워크 트래픽 분석에 기반한 이상증후 탐지 방식이므로, 일반적으로 이상증후 탐지 기반의 알고리즘들이 갖는 단점은 존재한다. 즉, signature 기반 탐지가 아닌 트래픽 기반의 탐지이므로, 이상 증후 감지 후 수작업으로 어떤 공격이었는지를 상세분석하는 것이 필요하다. 하지만, 현재까지 SCADA 제어망에 대한 공격패턴이 거의 알려져 있지 않은 상황에서는 이상증후 기반 탐지를 하는 것이 더 적합한 상태라 생각되고, 기존 시스템에 영향을 주지 않으면서 탐지를 해내는 기법인 본 연구가 큰 의미를 가지고 있다고 판단된다.

탐지된 위협에 대한 효과적인 대응을 위해서는 정상 탐지 여부를 판단하고 분석할 수 있는 전문인력과 특정 네트워크에서 발견된 패턴을 빠르게 타 네트워크로 전파할 수 있는 정보공유체계, 유관기관과의 협조를 통한 발빠른 행정조치 등이 절실히 요구된다.

최근 수년 간 스턱스넷 등 SCADA 망에 대한 공격 위협은 급속도로 증가하고 있고, 이에 대응하는 보안시스템이 거의 없는 상황에서 기존 SCADA 환경에서도 충분히 활용 가능한 침입탐지 모델의 연구는 우리 기반시설 운영 환경에 맞는 대안으로서 국가 인프라를 보호하는데 효과적인 도구로서 활용되리라 기대한다.

〔그림 6〕 종합 보안위협 대응체계 구성(안)

VII. 결 론

본 논문에서는 지하철, 수도, 교통 등 도시기반시설에서 운영 중인 SCADA시스템에 대한 위협 및 취약점 분석을 통해 위험도 분석했으며, 위험도를 최소화하고 SCADA시스템의 가용성을 확보된 상태에서 가장 효율적으로 위험을 측정할 수 있는 네트워크기반의 탐지모델 구현하였다. 취약점을 사전에 파악하고 있음에도 쉽게 조치할 수 없는 기반시설의 특성을 고려한 위험탐지 및 모니터링 모델은 타시도 및 정부기관에서 활용할 수 있을 것으로 기대된다. 단지, 네트워크모니터링 모델에 대해서는 보다 자동화되고 효율적인 알고리즘 개발과 현장 시스템에 적용될 수 있도록 추가적인 연구가 필요하다. 이 논문에서 제시하고 있는 것은 도시기반시설에 대한 직접 현장 실사한 데이터와 가용성 보장과 같은 SCADA시스템의 운영특성을 고려해서 가장 효율적인 네트워크 모니터링 제시 했다는 것에 큰 의미가 있다고 할 것이다.

참고문헌

〔1〕 Keith Stouffer, Joe Falco, and Karen Scarfone, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, Special Publication 800-82, Sep. 2008.

〔2〕 안철수연구소, "Stuxnet과 AhnLab TrusLine," Stuxnet White Paper ver. 1.0, pp. 3-6, 2010년 10월.

〔3〕 ISO/IEC 2000, "INTERNATIONAL STANDARD ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements," Oct 2005.

〔4〕 김휘강, "RFM 분석 방법론을 통한 지능적인 서버 기반 침입탐지 시스템", 석사학위 논문, 한국과학기술원, 1999년 12월.

〔5〕 Huy Kang Kim, Kwang Hyuk Im, and Sang Chan Park, "DSS for computer security incident response applying CBR and collaborative response," Expert Systems with Applications, Vol 37, Issue 1, pp. 852-870, Jan, 2010

〔6〕 Cheung, S., Dutertre, B., Fong, M.,

Lindqvist, U., Skinner, K., and Valdes, A., "Using model-based intrusion detection for SCADA network" In Proceedings of the SCADA Security Scientific Symposium, pp. 127-134 , Jan, 2007.

〔7〕 Verba, J. and Milvich, M., "Idaho national laboratory supervisory control and data acquisition intrusion detection system (SCADA IDS)", Technologies for Homeland Security, 2008 IEEE Conference on 12-13, pp.469-473. May 2008.

〔8〕 Holbert, K.E., Mishra, A., and Mili, L., "Intrusion Detection Through SCADA Systems Using Fuzzy Logic-Based State Estimation", International Journal of Critical Infrastructures, Vol. 3, No. 1-2, pp 58-87, Jan., 2007.

〔9〕 P. Oman and M. Phillips, "Intrusion detection and event monitoring in SCADA networks", in Critical Infrastructure Protection, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 161 - 173, Nov., 2007.

〔10〕 Tanya Roosta, Dennis K. Nilsson, Ulf Lindqvist, and Alfonso Valdes, "An Intrusion Detection System for Wireless Process Control Systems, Proceedings of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pp. 866 - 872, Sep., 2008.

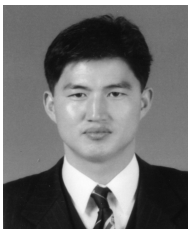
〔11〕 Andrea Carcano, Igor Nai Fovino, Marcelo Masera and Alberto Trombetta, "State-Based Network Intrusion Detection systems for SCADA protocols A proof of concept", Lecture Notes in Computer Science, Vol. 6027/2010, pp.138-150, Jul., 2010.

〔12〕 SPC basic charts: https://controls.engin.umich.edu/wiki/index.php/SPC:_Basic_control_charts:_theory_and_construction,_sample_size,_x-bar,_r_charts,_s_charts

〔13〕 RFM analysis,

〔14〕 http://en.wikipedia.org/wiki/RFM

〈著者紹介〉



김 완 집 (Wanjib Kim)
1992년 2월: 숭실대 전기공학 졸업(공학사)
2005년 9월: 성균관대 정보통신대학원 졸업 (석사)
2008년~현재: 순천향대학교 정보보호대학원 박사과정 재학 중
2006~현재: 서울시청 정보통신담당관 정보보호정책팀장
2011~현재: 행정안전부 정보보호정책 자문위원
〈관심분야〉 정보보호정책, 유·무선보안, 디지털포렌식

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

김 휘 강 (Huy Kang Kim)
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월 ~ 2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월 ~ 현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직

염 흥 열 (Heung-Youl YOUM)
1981년 2월: 한양대학교 전자공학과 학사 졸업
1983년 2월: 한양대학교 대학원 전자공학과 석사 졸업
1990년 2월: 한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소장
2000년 4월~2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 논문지편집위원 위원장, 수석부회장(역), 학회장(역)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신 연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재: ITU-T SG17 부의장 / SG17 WP2 의장
〈관심분야〉 인터넷보안, USN보안, IPTV보안, 홈네트워크 보안, 암호 프로토콜