비정상 네트워크 접근 탐지를 위한 전력 시스템 상태 모니터링 설계

김혁, 나중찬
과학기술연합대학원대학교 정보보호공학전공
한국전자통신연구원 사이버융합보안연구단
e-mail: hyukya@ust.ac.kr

The Design of Monitoring Power System States for Invalid Network Access Detection

Hyuk Kim, Jung-Chan Na
Information Security Engineering, University of Science and Technology
Cyber Security-Convergence Research Department, ETRI

요 약

전력시스템은 외부 망과 독립적으로 운영되는 폐쇄 망에서 점차 외부 망과의 연계됨으로써 외부 요소에 의한 위협, 다차원적인 시스템 취약성에 노출되고 있다. 서비스 거부 공격은 전력시스템에 매우 치명적이기 때문에 가장 중요한 가용성을 확실히 보장하기 위한 시스템과 네트워크의 운영 및 관리를 통한 보안 대책이 필요하게 되었다. 기존의 네트워크 트래픽만으로 분석하여 이상징후를 탐지하는 방식에 한계가 있기 때문에 본 논문에서는 전력시스템의 네트워크 상태와 엔드 시스템 상태 특성을 실시간 모니터링하고 분석하여 비정상 네트워크 접근을 탐지할 수 있는 시스템을 설계하였다.

1. 서론

SCADA(Supervisory Control and Data Acquisition)시스템은 외부 망과 독립적으로 운영되는 폐쇄 망이라는 인식은 SCADA시스템의 내부 업무 망을 통한 외부 연결 사례 및 이동 매체에 의한 스턱스넷과 같은 신종 악성코드 감염 사례 등에 의해 재조명되고 있다. 전력시스템이 점차 운영상의 이유로 외부 망과의 연계가 이루어지고, 나아가 스마트그리드가 도입됨으로써 전력 공급자와 소비자간 양방향 정보 교환이 가능한 IT융합 전력망을 구성하게 되면서 외부 요소에 의한 위협 유입, 다차원적인 시스템 취약성과 같은 보안문제에 노출되고 있다.

보통 가용성은 서비스 거부 공격을 통해 훼손되는데, 가용성 훼손은 시스템 자원이 의도적 또는 비의도적으로 소모됨으로써 해당 시스템의 마비, 불능 상태를 초래할 수 있다. 전력시스템이 서비스 거부 공격으로 인해 마비, 불능 상태가 된다면 제어 센터의 대응 불가, 전력 서비스 불가, 시스템 접근 불가 등 심각한 결과가 나타날 수 있기 때문에 가용성 확보가 필수적으로 이루어져야 한다. 가용성 보장이 최우선적 고려되는 전력시스템 환경에서는 데이터 전송 시간, 감지, 정보 제공 등의 시간 지연이 신뢰성을 위해 엄격하게 지켜져야 하며 이는 기존 IT시스템의 무결성, 기밀성 측면보다 중요성이 매우 크다[1].

전력시스템의 가용성 및 보안 안전성 확보를 위해서는 시스템 특성에 따른 보안 요구사항을 분석하고 보안 요구사항에 따른 보안 구조를 설계, 보안 대책 마련하는 프로세스가 확립되어야 한다[2]. 내부 공격에 의한 위협에 대응하기 위해서는 정상행위를 정의하고 이를 위배하는 행위를 이상징후로 판단하는 화이트리스트 기반 이상징후 감시시스템이 운영되어야 한다[3]. 또한 외부와의 통신 연결 접점을 통한 공격을 감지하고 대응하기 위한 침입감지시스템이나 침입방지시스템을 도입할 수 있다. 하지만 폐쇄적인 망 구성 정책은 내부 망의 안전성을 맹신하게 하였고 IT기술의 도입으로 인해 발생될 공격에 무방비하게 만들었기 때문에 앞에서 제시한 방법들을 제어 시스템에 적용하여 가용성 확보와 보안성 향상을 이끌어내야 한다. IEC 62351 표준에서는 전력망을 위한 정보 보안 기술을 제공하고 있으며, 특히 네트워크 및 시스템 관리를 통한 보안에 초점을 맞추고 있어 네트워크와 시스템의 지속적인 모니터링을 통해 전력시스템의 보안성을 높일 수 있도록 가이드하고 있다[4].

본 논문에서는 전력시스템 환경에서 네트워크 및 시스템 상태를 실시간 모니터링하여 수집된 데이터를 분석하여 비정상 네트워크 접근을 탐지는 방법을 제안하고자 한다. 본 논문의 2장에서는 관련 연구를 소개하고, 3장에서는 모니터링 구조와 전력시스템의 상태를 설계하고 비정상 네트워크 접근 탐지를 위한 모듈간 상호작용 과정을 기술한다. 마지막으로 4장에서 결론을 맺는다.

• 본 연구는 지식경제부의 재원으로 한국산업기술평가관리원(KEIT)의 지원을 받아 수행한 산업융합원천기술개발사업 입니다.(No. 10041560)

2. 관련 연구

침입탐지를 위한 방법으로는 데이터 마이닝, 시계열 분석 등을 사용하고, 탐지 대상 공격으로는 DoS 공격, 이상징후 등이 있다. 데이터 마이닝을 이용한 침입탐지 방법은 시스템의 자원을 고갈하는 대표적인 방법인 SYN 플러딩 공격과 버퍼 오버플로우 공격 등의 DoS 공격 유형을 탐지하기 위해 패킷 트래픽 통계 데이터 (패킷 수, 패킷 크기, 패킷 분포 등)와 시스템 정보 데이터(CPU, 메모리, 버퍼 등)을 결정 트리 알고리즘을 수행하여 보다 적은 수의 데이터 속성 모델링으로 탐지하는 시간을 줄일 수 있음을 보였다[5].

네트워크 트래픽을 대상으로 통계적 관점으로 DDoS와 같은 공격이나 이상징후 탐지를 위해서 시계열 기반 자기 유사성을 이용한 침입 탐지 연구들을 제안하였다[6,7]. SCADA 시스템 환경에서의 네트워크 트래픽은 규칙적이고 반복적인 특징을 보이기 때문에 자기 유사성 기반 침입탐지 방법을 적용하는 것이 매우 효과적임을 보였다. 정상 트래픽에 대한 코사인 유사성을 측정한 결과와 실제 공격 상황에서의 패킷을 수집하여 측정한 코사인 유사성 결과의 변화를 비교함으로써 공격의 증후를 감지할 수 있음을 보였다. 네트워크 트래픽 볼륨, 프로토콜별 비율을 선택하여 자기 유사성을 측정함으로써 다양한 네트워크 트래픽 특성을 통한 탐지가 가능하다는 것을 보여주었다.

컴퓨터 시스템 자원들의 소비 상태를 관찰하고 측정함으로써 앞으로 일어날 사건과 상태 변화를 예상하고 위험성을 탐지하기 위해서 컴퓨터 시스템 상태 모형을 사용한 방법을 제안하였다[8].

위에서 살펴본 연구들은 네트워크 트래픽을 실시간으로 모니터링하고 데이터를 모델링하는 탐지 과정을 수행하는 탐지방법을 제안하고 있지만, 주로 네트워크 트래픽 특성만을 관심가지고 있는 등의 단점을 가지고 있다. 네트워크 트래픽 특성만을 측정하여 침입탐지를 수행한다는 점에서 네트워크에 특이한 변화가 없는 공격을 탐지할 수 없다는 한계가 있다. 따라서 이러한 한계를 극복하기 위해서는 시스템 상태를 측정함으로써 위협을 탐지하는 기법을 전력시스템에 적용하여 신뢰성 있는 탐지할 수 있는 방법이 필요하다.

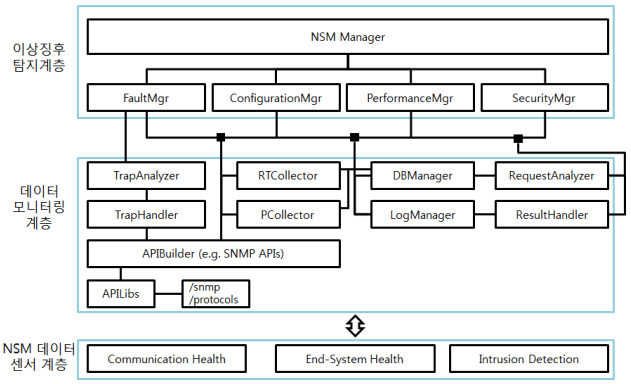
3. 시스템 설계

전력시스템은 크게 네트워크와 엔드 시스템으로 구성되어 있다. 네트워크에는 통신 네트워크 구성, 통신 프로토콜, 네트워크 성능 등이 포함되며 엔드 시스템에는 IED(Intelligent Electronic Device), RTU(Remote Terminal Unit) 등이 포함된다. 이러한 시스템 운영의 보안과 신뢰성 확보를 위해 IEC 62351-7에서는 NSM (Network and System Management) 데이터 객체 모델을 정의하였다[9].

NSM 데이터 객체를 사용하여 전력시스템의 상태를 모니터링하기 위해서는 네트워크와 시스템에 맞는 NSM 데이터 객체로 알맞게 배치되어야 한다. *Communications Health* 객체의 경우 네트워크와 프로토콜과 관련되어 있으므로 네트워크 상태를 모니터링하는데 사용될 수 있으며, *End System Health* 객체의 경우 엔드 시스템과 관련되어 있으므로 시스템 상태를 모니터링하는데 적합한 데이터 객체이다. 또한 *Intrusion Detection* 객체의 경우에는 네트워크 및 시스템 전체에 걸쳐 침입 탐지하는데 사용되는 객체이기 때문에 해당 객체는 양쪽에 걸쳐 사용될 수 있다.

3.1. 시스템 구조

비정상 네트워크 접근을 탐지하기 위한 시스템의 구조는 (그림 1)과 같다.



(그림 1) 시스템 구조

시스템은 크게 이상징후 탐지 계층, 데이터 모니터링 계층, NSM 데이터 센서 계층으로 구성되어 있고 계층 별 기능은 다음과 같다.

- 이상징후 탐지 계층
  장애분석, 구성관리, 성능분석이나 NSM MIB 분석을 통해 비정상 네트워크 접근을 탐지
- 데이터 모니터링 계층
  NSM MIB과 트랩 메시지를 실시간 수집하고 처리
- NSM 데이터 센서 계층
  전력 설비 및 보안 센서에서 발생하는 이벤트를 NSM MIB 형태로 가공 및 전달

그리고 각 계층은 여러 개의 기능 모듈로 구성되어 있다. 이상징후 탐지 계층은 NSM 매니저(*NSM Manager*), 장애관리(*FaultMgr*), 구성관리(*ConfigurationMgr*), 성능관리(*PerformanceMgr*), 보안관리(*SecurityMgr*) 모듈로 구성되어 있으며 모듈별 기능은 아래와 같다.

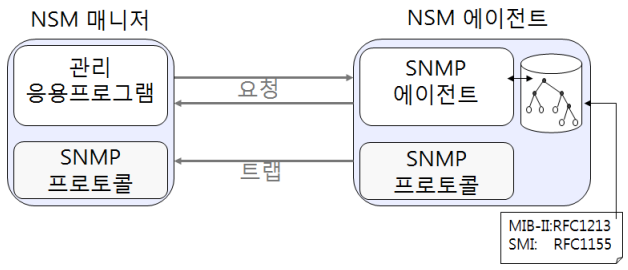
- NSM 매니저 기능
  수집된 NSM MIB이나 분석된 자료를 통해 비정상 네트워크 접근을 탐지하는 기능
- 장애관리 기능
  네트워크 및 엔드 시스템에서 발생하는 장애를 전달 및 처리하는 기능
- 구성관리 기능
  관리 대상 네트워크 및 엔드 시스템에 대한 구성 설정과 관리 정책을 통해 감시 및 관리하는 기능
- 성능관리 기능
  수집된 MIB을 분석하여 시스템의 가용성, 응답시간, 부하 및 성능 정도를 분석하고 통계 정보를 생성하는 기능
- 보안관리 기능
  시스템에서 발생하는 다양한 보안 이벤트를 통해 비정상 네트워크 접근을 탐지하는데 지원하는 기능

데이터 모니터링 계층은 NSM 데이터 센서 계층에서 발생하는 이벤트를 안정적으로 처리할 수 있도록 수집, 저장, 정규화하는 등의 처리 기능을 수행한다. 각 모듈 별 수행하는 기능은 다음과 같다.

- TrapAnalyzer: 트랩 이벤트 분석
- TrapHandler: 트랩 이벤트 수집 및 처리
- RTCollector: 실시간 NSM MIB 수집
- PCollector: 주기적 NSM MIB 수집
- DBManager: 데이터베이스 저장 기능
- LogManager: 로그 관리 기능
- RequestAnalyzer: 요청 분석 기능
- ResultHandler: 에러 체크 등 요청 처리 기능
- APIBuilder: SNMP APIs의 생성자

3.2. NSM 데이터 수집 및 통지를 위한 구조

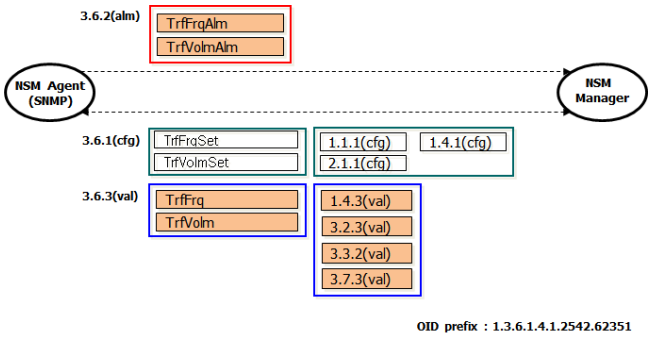
전력 시스템의 네트워크와 엔드 시스템 상태를 지속적으로 모니터링하기 위한 NSM 매니저-에이전트 구조는 (그림 2)와 같다.



(그림 2) NSM 매니저-에이전트 구조

위 구조는 매니저와 에이전트 간에는 SNMP 프로토콜을 통해 요청 및 트랩을 전송하는 것을 보여주고 있다. NSM 매니저는 데이터 모니터링 계층을 통해 NSM 에이전트로부터 발생하는 NSM 데이터 알람을 수집하고 처리하며, 에이전트에게 NSM MIB 데이터를 요청하여 값을 수집하거나 설정할 수 있다. NSM 에이전트는 전력 설비 및 보안 센서에서 발생하는 엔드 시스템의 상태 이벤트를 업데이트하고 매니저의 요청에 응답하거나 상태 변화 발생 시 알람을 발생시킨다.

매니저에서 비정상 네트워크 접근을 탐지하는데 가장 관심을 가지는 NSM 객체는 알람 데이터 객체이며, 요청하고 분석해야 하는 객체는 구성이나 값과 관련된 정보들이다. (그림 3)은 비정상 네트워크 접근을 탐지하는데 수신되는 알람 데이터 객체는 트래픽 주기 초과를 나타내는 *TrfFrqAlm*, 트래픽 볼륨 초과를 나타내는 *TrfVolmAlm*이고, 수신된 알람을 입증하기 위해 *TrfFrqSet*, *TrfVolmSet*, *TrfFrq*, *TrfVolm* 등과 같은 데이터 객체를 활용할 수 있음을 보여준다.



(그림 3) 비정상 네트워크 접근 관련 데이터 객체

3.3. 상태 특성과 NSM 객체 간 매핑

비정상 네트워크 접근은 주로 서비스 거부 공격에 의해 발생할 수 있으며, 서비스 거부 공격이 영향을 미치는 네트워크와 엔드 시스템 상태에는 초당 패킷 수(PPS), 초당 바이트 수(BPS), 평균 패킷 크기, 버퍼 사용량, CPU 사용률, 자원 사용률 등이 있다.

<표 1> 상태 특성과 NSM MIB 매핑

상태 특성		*OID	NSM MIB	설명	
초당 패킷 수	⇔	3.6.1.1	*TrfFrqSet*	최대 트래픽 주기 세팅	네트워크
		3.6.3.1	*TrfFrq*	트래픽 주기	
초당 바이트 수	⇔	3.6.1.2	*TrfVolmSet*	최대 트래픽 양 세팅	
		3.6.3.2	*TrfVolm*	트래픽 양	
평균 패킷 크기	⇔	1.4.3.5	*MsgBytAv*	평균 메시지 바이트 크기	
버퍼 사용량	⇔	3.3.2.1	*BufOvCnt*	버퍼 오버런 발생 횟수	엔드 시스템
CPU 사용률	⇔	3.2.3.3	*IdlTmms*	실제 유휴 시간	
자원 사용률	⇔	1.4.1.3	*RescExhPct*	자원 사용 비율	

* OID prefix: 1.3.6.1.4.1.2542.62351

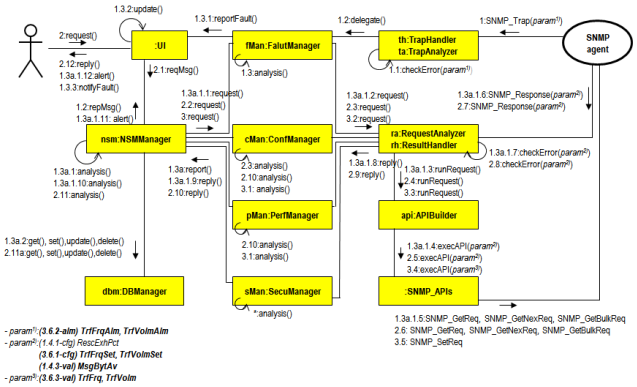
이와 같은 전력시스템의 네트워크 상태와 엔드 시스템 상태와 매핑되는 NSM MIB은 <표 1>과 같다. 각 상태 특성들은 NSM 데이터 객체와 1:N으로 매핑될 수 있다.

네트워크 상태와 관련된 *TrfFrq*, *TrfVolm*, *MsgBytAv*은 각각 초당 패킷 수, 초당 바이트 수, 평균 패킷 크기를 나타낸다. 추가적으로 *TrfFrqSet*과 *TrfVolmSet*은 초당 패킷 수와 초당 바이트 수의 최대치를 설정하는 값으로써 네트워크 상태를 나타내는데 활용될 수 있다.

그리고 엔드 시스템과 관련된 BufOvCnt, IdlTmms, RescExhPct는 각각 버퍼 오버런 발생 횟수, 실제 유휴 시간, 자원 사용 비율을 나타내며 엔드 시스템의 상태를 파악하기 위한 데이터로 활용된다.

3.4. 모니터링 설계를 위한 상호작용 다이어그램

(그림 4)는 상태를 모니터링하고 비정상 네트워크 접근을 탐지하기 위한 분석을 수행하는데 참여하는 클래스 간 상호작용을 정의하는 상호작용 다이어그램이다.



(그림 4) 모듈 간 상호작용 다이어그램

NSM 매니저는 액터와 NSM 에이전트와 메시지를 주고받으며 상호작용하며, 액터나 매니저가 에이전트에 요청하거나 에이전트가 요청에 대한 응답, 트랩을 전송하는 메시지 교환이 주로 이루어질 때 메시지에 대한 에러, 응답 데이터의 분석을 수행한다. (그림 4)는 비정상 네트워크 접근을 탐지하는 시나리오의 예로써, 에이전트에서 시스템으로 트랩 메시지를 전송하고 액터가 이를 수신하는 과정(*1:SNMP_Trap(param)*), 액터가 관련 NSM 데이터를 요청하고 응답을 분석하는 과정 (*2:request()*) 그리고 nsm:*NSMManager* 오브젝트가 구성, 성능, 보안관리 기능을 분석하고 에이전트를 올바르게 설정하는 과정 (*3:request()*)을 보여준다.

4. 결론

본 논문에서는 가용성 확보를 위하여 전력시스템의 네트워크 상태뿐만 아니라 엔드 시스템의 상태를 분석함으로써 비정상 네트워크 탐지 시스템을 설계하였다. 전력시스템의 네트워크와 엔드 시스템의 상태를 IEC 62351-7 표준에 따라 추출하고, 각 상태 정보들을 실시간으로 모니터링하고 연관성을 분석하여 비정상 네트워크 접근을 탐지할 수 있다. 탐지를 수행하는데 사용된 NSM MIB은 각 상태 정보들과 매핑하여 네트워크 및 엔드 시스템의 상태를 관측하는데 활용하였다. 그리고 관리자 또는 사용자와 매니저, 에이전트간의 데이터 교환 과정을 다이어그램을 통해 보여주었다.

앞으로 본 연구에서 설계한 모니터링 시스템을 구현한 결과를 통해 전력 시스템에서의 비정상 네트워크 접근 탐지 성능을 보여줄 수 있을 것이다.

참고문헌

[1] NIST, “NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements” August, 2010

[2] 전용희 “스마트 그리드의 취약성, 특성, 설계 원칙 및 보안 요구사항 분석” 정보보호학회지 제20권 제3호, 6월, 2010

[3] 최문석, 임용훈, 주성호 “전력 제어시스템 보안성 향상에 관한 연구” 2011 한국정보기술학회 하계학술대회 논문집

[4] 권기풍, 서승우 “지능형 전력망을 위한 정보 보안” 전기의 세계 제58권 제 8호, 8월, 2009

[5] Kyung Choi, Xinyi Chen, Shi Li, Mihui Kim, Kijoon Chae and JungChan Na “Intrusion Detection of NSM Based DoS Attacks Using Data Mining in Smart Grid” Energies, 5(10), 2012

[6] Y.Xiang, Y.Lin, W.L. and S.J. Huang “Detection DDOS attack based on network self-similarity” IEE Proceedings-Communications, June, 2004

[7] 고폴린, 최화재, 김세령, 권혁민, 김휘강 “트래픽 자기유사성에 기반한 SCADA 시스템 환경에서의 침입탐지 방법론” 정보보호학회논문지 제22권 제2호, 4월, 2012

[8] 곽미라, 조동섭 “시스템 상태 모형을 사용한 위협 탐지 기법” 2006년도 대한전기학회 하계학술대회 논문집 2006

[9] IEC/TS 62351-7, “Power Systems Management and associated information exchange - Data and Communications Security - Part 7 : Network and System Management(NSM) data object models“ 2009