2019년 2월

석사학위 논문

스마트그리드 환경에서 보안을 위한 온톨로지 기반 공격탐지 기법

조선대학교 산업기술융합대학원

소프트웨어융합공학과

김 기 훈

2019년 2월

석사학위논문

스마트그리드 환경에서 보안을 위한 온톨로지 기반 공격탐지 기법

김 기 훈

스마트그리드 환경에서 보안을 위한 온톨로지 기반 공격탐지 기법

Ontology-based Attack Detection for Security in Smart Grid Environments

2019년 2월 25일

조선대학교 산업기술융합대학원

소프트웨어융합공학과

김 기 훈

스마트그리드 환경에서 보안을 위한 온톨로지 기반 공격탐지 기법

지도교수 최 준 호

이 논문을 공학석사학위신청 논문으로 제출함.

2019년 2월

조선대학교 산업기술융합대학원

소프트웨어융합공학과

김 기 훈

김기훈의 석사학위논문을 인준함

위원장 조선대학교 교수 김 판 구 (인)

위 원 조선대학교 교수 신 주 현 (인)

위 원 조선대학교 교수 최 준 호 (인)

2018년 11월

조선대학교 산업기술융합대학원

목 차

ABSTRACT

Ⅰ. 서론 ····· 1
A. 연구 배경 및 목적 ····· 1
B. 연구 내용 및 구성 ····· 3

Ⅱ. 관련 연구 ····· 4
A. 전력 시스템의 보안 위협 현황 및 탐지 방법 ····· 4
B. 온톨로지 기반 추론기술 ····· 8
C. 지능형 접근제어 기술 ····· 11

Ⅲ. 스마트그리드 보안을 위한 온톨로지 기반 공격탐지 기법 ····· 13
A. 전력 시스템의 보안을 위한 전체 시스템 구성도 ····· 13
B. 전력 시스템의 보안을 위한 시스템 취약점 분석 ····· 15
C. 공격 탐지를 위한 온톨로지 구축 및 추론규칙 설계 ····· 24

Ⅳ. 실험 및 평가 ····· 32
A. 공격 상황 시나리오 구성 ····· 32
B. 시나리오 정보에 기반한 공격 상황 추출 ····· 33
C. 시나리오 정보에 기반한 공격 상황 탐지 ····· 35

Ⅴ. 결론 및 제언 ····· 38

참고문헌 ····· 39

표 목 차

[표 2-1] 스마트그리드 보안 위협 요소 ····· 4
[표 2-2] 스마트그리드 전력 시스템 공격 행위 ····· 5
[표 2-3] 국내 스마트그리드 보안 과제 연구내용 ····· 7
[표 2-4] 온톨로지 구성요소 ····· 8
[표 2-5] SWRL 기본 규칙 및 규칙 예제 ····· 10
[표 2-6] 주요 접근통제 방식 구분 ····· 12
[표 3-1] SCADA 시스템의 취약점 분석 ····· 16
[표 3-2] EMS 시스템의 취약점 분석 ····· 18
[표 3-3] MDMS 시스템의 취약점 분석 ····· 20
[표 3-4] 스마트 미터에 가해지는 공격 행위 ····· 21
[표 3-5] 스마트 미터 취약점 분석 ····· 22
[표 3-6] 스마트 미터 취약점 세부 분석 ····· 22
[표 3-7] Level 2와 Level 3클래스 정의 ····· 25
[표 3-8] Level 3부터 Level 5까지의 클래스 정의 ····· 27
[표 3-9] 주요 Property 정의 ····· 28
[표 3-10] 물리적·네트워크적 공격단계 추론규칙 ····· 29
[표 3-11] 시스템 접근단계 추론규칙 ····· 30
[표 3-12] 시스템 조작단계 추론규칙 ····· 30
[표 3-13] 온톨로지를 통한 객체간 관계 표현 ····· 31
[표 4-1] 상황 시나리오 ····· 32
[표 4-2] 공격상황 추출 및 클래스 정의 ····· 33
[표 4-3] 공격 상황 탐지 추론식 ····· 35
[표 4-4] 시스템 구현 환경 ····· 36
[표 4-5] 상황별 추론 인식 여부 ····· 37

그 림 목 차

[그림 1-1] 다양한 분야의 사이버 공격 ····· 1
[그림 2-1] 스마트그리드 실증단지 보안 대책 개념도 ····· 6
[그림 2-2] 시맨틱 웹 아키텍처 ····· 9
[그림 2-3] 접근 통제 절차 ····· 11
[그림 3-1] 전체 시스템 구성도 ····· 13
[그림 3-2] 온톨로지 추론과정 프로세스 ····· 14
[그림 3-3] SCADA 시스템 구성요소 ····· 15
[그림 3-4] EMS 시스템 구성요소 ····· 17
[그림 3-5] MDMS 시스템 구성요소 ····· 19
[그림 3-6] 기본 클래스 관계도 ····· 24
[그림 3-7] 전력 시스템 온톨로지 관계도 ····· 26
[그림 3-8] Metering System 관계도 ····· 27
[그림 3-9] 상황추론 진행 과정 ····· 31
[그림 4-1] SWRL 추론식 실행 결과 ····· 36

ABSTRACT

Ontology-based Attack Detection for Security in Smart Grid Environments

Gihoon Kim
Advisor : Prof. JunHo Choi, Ph.D
Department of Software
Convergence Engineering
Graduate School of Industry
Technology Convergence,
Chosun University.

The concept of the Smart Grid has emerged to solve this problem due to exhaustion of natural resources and environmental problems worldwide. Smart Grid is a convergence technology that combines Smart and Grid with distributed power systems, which is a core concept and exchange real-time information between suppliers and consumers with ICT (Information Communication Technology) technology. While the smart grid industry is active in countries around the world to expand renewable energy sources and ensure stable power operation, there is a potential for security threats to attack related vulnerabilities by spreading and expanding a variety of core devices.

Smart Grid technology has the advantage of maximizing energy efficiency by utilizing two-way communication technologies in power systems, but since it has an open-ended structure unlike traditional suppliers and consumers, it can easily be exposed to various forms of cyber attacks.

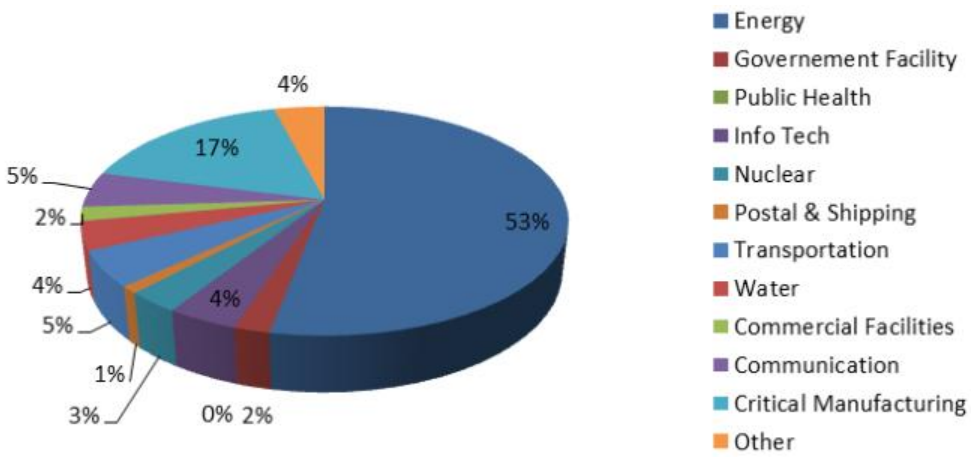
These various attacks are likely to cause major damage to the nation, and an intelligent security control system is expected to be needed as a counter-attack. An intelligent security control system could detect and analyze various invasions and take quick action.

To this end, this paper proposed an ontology-based attack detection technique for Smart Grid Security. The proposed method is to collect, analyze, and categorize the security vulnerabilities of the power system and apply the inference engine to the major power systems to identify and respond early in the event of an attack.

Ⅰ. 서론

A. 연구 배경 및 목적

스마트그리드는 지능형(Smart)과 전력망(Grid)이 합쳐진 융·복합 기술로써 분산 전원 시스템을 핵심 개념으로 기존 전력망에 ICT(Information Communication Technology)기술을 접목해 공급자와 소비자간의 실시간 정보를 양방향으로 교환하는 분산·개방형 아키텍처의 구조를 가지고 있다[1]. 양방향 소통기술을 활용해 에너지 효율의 최적화를 극대화 시킬 수 있다는 장점이 있지만, 기존의 전력망과는 다르게 개방형 구조를 가지고 있기 때문에 다양한 형태의 사이버 공격에 쉽게 노출될 수 있고, 인접한 다른 전력 시스템의 취약점을 파고들어 국가적인 큰 피해를 입힐 수 있다는 단점이 있다.



[그림 1-1] 다양한 분야의 사이버 공격[2]

다양한 분야의 사이버 공격 발생률을 [그림 1-1]로 나타내었다. 전력 시스템의 발생률이 월등히 높음을 알 수 있으며, 관련 전력 시스템의 보안 위협 상황에 대응하기 위해 여러 가지 보안 장비 및 관리체계를 활용하여 공격의 탐지 및 예방을 하고 있으나, 기존의 사이버 보안 기술로는 조기 식별 및 대응을 하기가 어려워 큰 피해를 입힐 수 있기 때문에 지능적인 식별 기술이 필요하다.

또한 산업통상자원부의 보고서에 의하면[3] AMI, ESS 등 스마트그리드 환경 구현을 위해 필수적인 핵심기기 보급을 활성화하여 스마트그리드 기반 구축을 추진하고 있기 때문에 기존의 취약점을 파고드는 공격이 더욱 심화될 것이라 전망된다.

따라서 본 논문에서는 스마트 그리드 시스템에 가해지는 공격 방식 및 상황 정보를 분석하고, 이를 기반으로 온톨로지를 구축해 관련 규칙을 설계하여 전력 시스템의 공격 탐지 기법을 제안하고자 한다.

B. 연구 내용 및 구성

본 연구의 주요 내용은 스마트그리드의 전력 시스템에 가해지는 공격 상황 정보를 기반으로 보안 온톨로지를 설계하며, 설계된 온톨로지를 기반으로 관련 규칙을 제정해 지능화된 접근제어 추론 기법 방안을 제안한다. 본 논문의 구성은 다음과 같다.

서론에 이어 2장에서는 온톨로지 설계의 이론적 배경이 되는 전력 시스템의 보안 위협 현황 및 탐지방법, 온톨로지 기반 추론 기술, 지능형 접근제어 기술에 대한 기존 연구에 대해 서술한다.

3장에서는 제안하는 온톨로지 기반의 공격 탐지모델 구축을 위한 전체 시스템 구성도와 시스템에 가해지는 공격 데이터를 수집 및 분석하고 추론규칙을 제정한 보안 온톨로지 구축 및 추론 설계에 대해 서술한다.

4장에서는 제정된 추론 규칙을 이용해 온톨로지를 구동하는 테스트를 해봄으로써 정상적으로 동작하는지를 확인하는 실험 및 평가단계이다.

마지막으로 5장에서는 결론과 향후 연구계획에 대해 서술하며 논문을 마무리한다.

Ⅱ. 관련 연구

A. 전력 시스템의 보안 위협 현황 및 탐지 방법

1. 스마트그리드 보안 위협

중앙 집중식 폐쇄적 단방향 통신 구조인 기존 전력망은 보안문제가 크게 대두되지는 않았으나, 스마트 그리드는 기존 전력망에 ICT 기술을 접목한 기술이기에 기존의 전력망에서 발생되지 않았던 네트워크 보안 문제가 드러나고 있다[4, 5, 6]. 기존에는 소비자 망에서 중앙으로의 정보제공이 필요하지 않았지만, 스마트그리드에서는 사용자의 요구사항의 관철을 위해 정보 획득을 필요로 하기 때문에 관련 통신기기 및 센서 네트워크 등의 보안취약점 문제와 시스템의 개방성으로 인한 인접 네트워크로 쉽게 침투할 수 있는 문제가 있다.

[표 2-1] 스마트그리드 보안 위협 요소

구분	내용
양방향 통신 서비스	양방향 통신기술을 사용함으로써, 공격 대상 및 위협 증가
상용 HW/SW 사용 증가	상용 제품을 사용함으로써, 기존에 알려진 취약점 노출
외부 연결접점의 증가	소비자 단의 접근 가능지점의 증가로 인해 공격자에게 다양한 침입 루트 제공
장비간 상호연결 증가	스마트그리드 장비간 상호연결의 증가로 인해 공격자의 침입 루트의 다양화
광범위한 지역의 장비 산재	광범위한 지역에 장비가 물리적으로 산재됨으로 인해 관리의 부재

[표 2-1]는 스마트그리드 관련 보안 위협 요소를 대분류하여 나타낸 것으로써 중요하게 다룰 내용은 외부 연결접점의 증가와 장비간 상호연결 증가이다. 전력 소비자 단에서 접근 지점의 증가와 스마트그리드 장비간 상호연결의 증가로 인해 공격자의 침입 루트가 다양화됨에 따라 수많은 보안 위협 요소들이 산재해 있다.

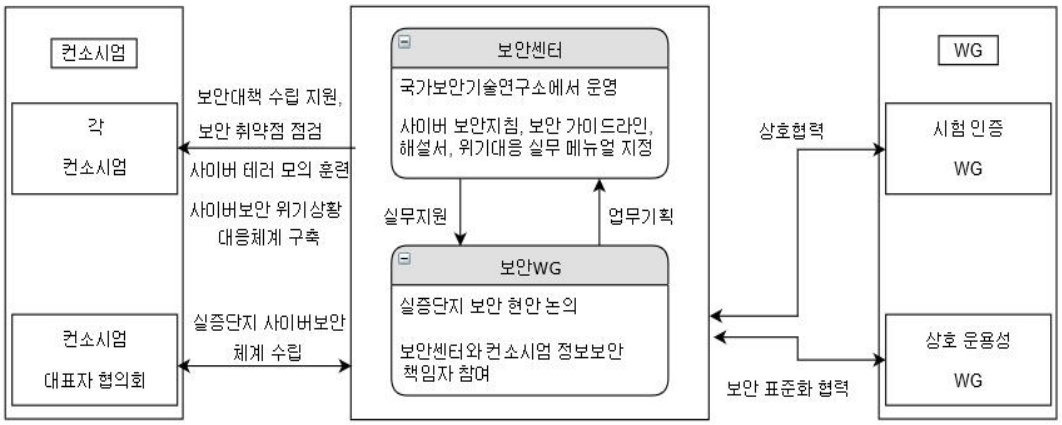
[표 2-2] 스마트그리드 전력 시스템 공격 행위

구분	내용
감청	시스템의 모든 부분에 적용될 수 있으며 필요한 인증 과정에 사용되는 암호를 알아낼 수 있음.
트로이 목마	웹 기반 엑세스를 통해 인증 정보를 탈취하거나 시스템을 오염시킬 수 있음.
백도어	표준화된 상용제품의 서버 및 기기들이 공급되며, 악의적인 백도어가 내장되어 공급될 수 있음.
서비스 위장	비인가된 접속이지만 인가를 받은 기기처럼 위장하여 잘못된 정보를 서버에 전송해 제어신호를 유도하거나, 시스템의 오류를 유도할 수 있음.
신분 위장	시스템의 일부로 위장하여 정보를 염탐하고, 오염시키거나, 시스템에 대한 공격을 준비함.
권한 위조	권한을 위조하여 허용된 정보보다 상위의 정보에 접근하고, 제어권을 획득하여 불법 조작을 할 수 있음.
물리적 침입	광범위한 지역의 장비 산재로 인해 모든 부분을 물리적으로 모니터링하기에는 한계가 있어 외부로부터의 접근을 허용할 수 있음.
Replay 공격	네트워크 프레임을 수집한 뒤 메시지를 재전송하여 미갱신 정보의 전달 혹은 정상정보로 위장시켜 오류를 유도할 수 있음.
서비스 거부	대량의 데이터 패킷을 보냄으로써 서버의 자원을 고갈시킬 수 있음

위의 [표 2-2]는 스마트그리드 전력 시스템의 보안 위협 요소를 이용해 공격이 발생하는 행위를 정리한 표이다[7]. 기존 전력망과 달리 공격의 종류가 다양해졌고, 이러한 공격은 심각한 국가적 피해를 초래할 수 있다. 다양한 위협들을 기준에 따라 분류하였으며, 표에서 서술한 공격 행위들을 바탕으로 전력 시스템에 지속적으로 일어나는 공격에 대한 명확한 판단 및 신속한 대응을 위해서는 통합적이고 지능적인 보안 기술이 필요하다.

2. 스마트그리드 보안위협 탐지방법

국내에서 시행하고 있는 제주 스마트그리드 실증단지에서는 국가보안기술연구소를 필두로 보안WG 및 보안센터를 운영하여 보안지침 및 가이드라인 제시, 운영센터별 보안대책 수립 등을 통해 보안 대책을 여러 각도로 마련하고 있다[8].



[그림 2-1] 스마트그리드 실증단지 보안 대책 개념도

제주 스마트그리드 실증단지에서의 개념체계를 도식화하여 [그림 2-1]과 같이 나타내었다. 스마트그리드 전력시스템의 보안취약점을 점검하고, 사이버 테러 모의훈련을 함으로써 보안 위협 상황에서의 대응체계를 구축하며, 이로인한 사이버보안 체계를 수립하게 된다. 보안 위협상황은 크게 두가지로 나누어 파악하게 된다.

운영 측면에서의 위협상황으로는 발생되는 외부의 침입, 웜과 백도어와 같은 악성코드 감염, 정보의 손상, 침입 전이 등을 식별한다.

스마트그리드 기기에서의 위협상황으로는 기기에 가해지는 침입공격, 악성코드 감염, 중요 정보의 손상, 기기 복제 등을 위협으로 고려한다.

이에 대한 보안 대책으로는 암호 알고리즘 목록 사용, 인증 및 키 관리, 운영센터에서의 관리적 보안, 스마트그리드 기기 보안대책 등이 있다. 이밖에도 정부지원 스마트그리드 보안과제들의 연구내용을 [표 2-3]에 나타내었다[8].

[표 2-3] 국내 스마트그리드 보안 과제 연구내용

구분	내용
보안플랫폼 연구	· 스마트그리드 보안모델링 · 스마트그리드 보안체계 확립
DDoS 공격인식 및 대응방법 개발	· 스마트그리드 환경에서 발생 가능한 DDoS 공격 패턴 연구 · DDoS 공격 전 악성행위의 확산을 탐지하고 저지하는 기술 개발 · DDoS 공격 발생 시 공격을 인식하고 차단할 수 있는 기술 개발
스마트그리드 기술연구	· 스마트그리드 보안위협 및 취약점 분석 · 스마트그리드 사전진단 및 안전진단 자동화 도구 개발 · 스마트그리드 사이버공격 및 이상징후 탐지기술 개발 · 스마트그리드 통합 모니터링 시스템 구축 및 공격 대응체계 수립 · 스마트 어플라이언스 키 교환 및 관리기법 설계 · 스마트 어플라이언스 인증기술 및 통합 프레임워크 개발 · 스마트 미터기 등에서 고객 프라이버시 보호기술 개발 · 개인정보 유출 방지를 위한 암호화된 데이터 검색 기술 개발
스마트그리드 핵심보안기술 개발	· 스마트그리드 보안 기반기술 연구개발 · 스마트그리드 보안 관제기술 연구개발 · 스마트그리드 기기 보안기술 연구개발

[표 2-3]과 같이 스마트그리드 보안 과제의 주요 연구내용을 나타내었다[8]. 보안체계 연구, 공격탐지 및 대응기술 개발, 기술연구, 핵심보안기술 개발의 네 단계로 구분되어진다. 세계 각국에서 스마트그리드 산업을 활성화시키고 있지만 각 나라의 환경에 맞게 보안체계를 추진하기 때문에 우리나라도 국내 환경에 적합한 스마트그리드 보안모델 체계를 연구중이다. 개발 연구로는 여러 가지 구성요소가 결합되어 있는 스마트그리드 환경의 특성상 보안을 위한 여러 방법들의 연구가 진행중이며, 하나의 시스템 항목들간의 기술연구를 결합하여 스마트그리드의 전체적인 핵심 보안 기술을 개발하게 된다.

B. 온톨로지 기반 추론 기술

IT 기술이 발달되고 다량의 데이터가 축적됨에 따라 불필요한 정보와 데이터들의 발생 비율이 크게 증가하고 있다. 의미있는 데이터를 추출하기 위한 시간과 비용이 함께 증가하게 되었고, 이를 해결하기 위한 온톨로지에 대한 연구가 다양하게 진행되고 있으며, 온톨로지의 궁극적인 목적은 컴퓨터가 처리할 수 있는 특정 영역의 지식체계를 모델링 함에 있다[9].

일반적으로 온톨로지는 도메인 내의 개념 및 개념 사이의 관계, 개념의 속성 및 특성, 속성 및 특성에 부여된 제약 조건 및 객체들로 표현되는 개념 계층 구조이다[10]. 이를 이용해서 특정 도메인의 단어를 공통으로 정의하고, 지식을 공유할 수 있으며 가장 큰 특징으로는 추론을 통해 기존의 데이터로부터 새로운 데이터를 생성해 지식베이스를 확장할 수 있다는 것이다.

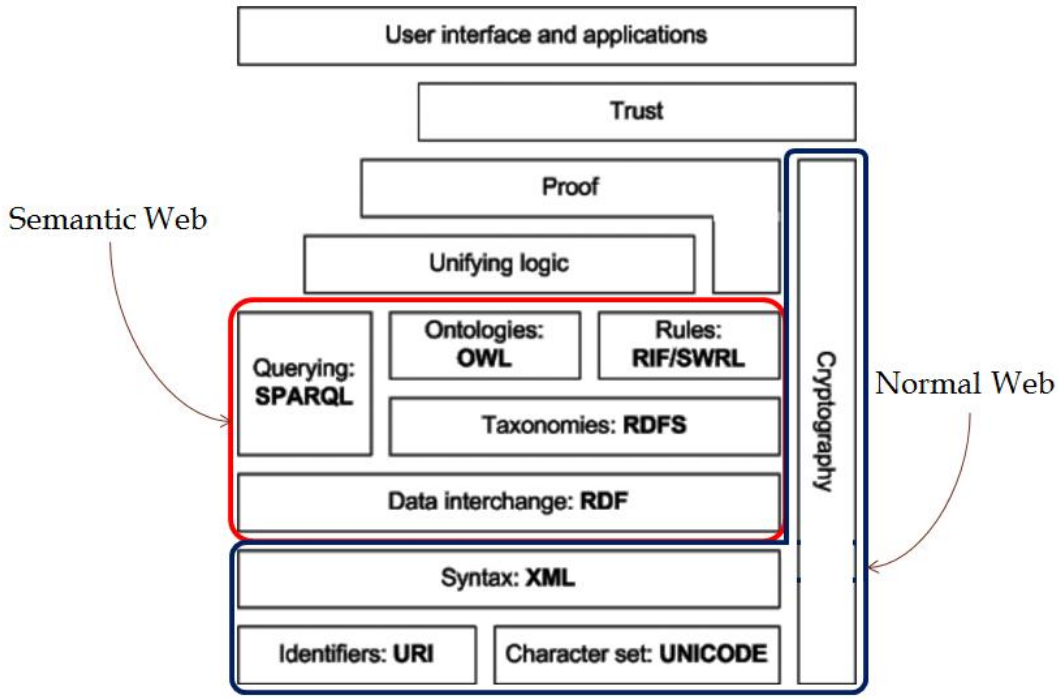
[표 2-4] 온톨로지 구성요소

구성요소	내용
클래스	영역에 존재하는 물리적·개념적 개체
관계	개체간의 연관성을 나타내며 클래스와 인스턴스간에 존재
인스턴스	온톨로지 구성요소중 개체의 실체가 있는 형태중 가장 수준이 낮은 요소
속성	개체들간의 관계이자 근본적인 성질
공리	제약값을 주기 위한 항상 참인 문장
규칙	특정 값에 따른 논리적 추론문장

온톨로지의 구성요소를 전반적으로 정리해 다음 [표 2-4]로 나타내었다. 온톨로지는 클래스(Class), 관계(Relationship), 인스턴스(Instance), 속성(Attribute), 공리(axiom), 규칙(rule)의 구성으로 이루어지며, 이러한 특성을 이용하여 다양한 웹 관련 분야에서 활용되고 있으며, 웹 데이터에 의미를 부여해 이를 해석하고 효율적인 공유를 할 수 있는 시맨틱 웹 기술의 핵심 요소이다.

온톨로지 개념을 웹에 적용하고 처리하고자 하는 웹을 시맨틱 웹이라고 한다.

[그림 2-2]는 시맨틱 웹을 전체적으로 표현한 아키텍처이며 온톨로지를 표현하는 웹 표준언어인 OWL(Web Ontology Langauge), 정보를 검색하는 SPARQL, 표현된 지식규칙을 제공해 추론을 가능하게 해주는 SWRL이 대표적이다.



[그림 2-2] 시맨틱 웹 아키텍처[11]

온톨로지에서의 추론 방법은 크게 기술 논리 기반의 추론과 규칙 기반의 추론의 두가지 방법으로 나누어지며 기술 논리기반의 추론기법은 추론 결과에 대한 정확성이 보장되지만 대용량의 추론에 있어 효율성이 떨어지는 단점이 있으며, 규칙 기반의 추론은 효율적인 규칙 적용을 통해 대용량의 온톨로지 처리에 유리한 이점을 지니고 있다[12]. 지식베이스 구축에 있어서 온톨로지의 유연한 시스템은 데이터의 최신성 유지 및 데이터의 유용성, 위협분석 정보 활용에 큰 이점이 주어진다. 본 논문에서는 추론을 위한 언어로 SWRL(Semantic Web Language)를 사용하여 규칙기반 추론을 하고자 하며 SWRL의 기본규칙 및 예제를 [표 2-5]에 나타내었다.

[표 2-5] SWRL 기본 규칙 및 규칙 예제

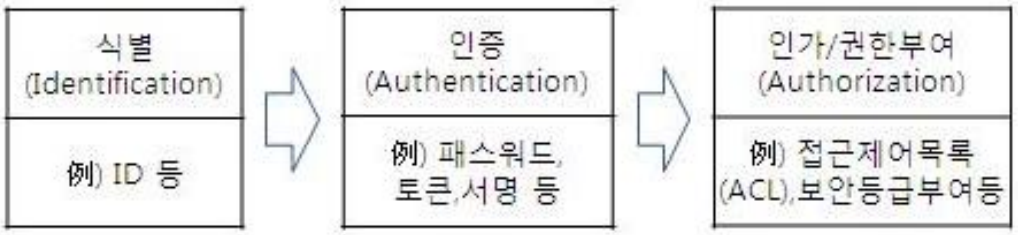
SWRL 기본 규칙
$hasProperty_1(?x, ?y) \wedge hasProperty_2(?y, ?z) \wedge .... hasProperty_n(?y, ?z) \Rightarrow$ hasFinal(?x, ?z)
SWRL 규칙 예제
hasParent(?x1,?x2) ∧ hasBrother(?x2,?x3) ⇒ hasUncle(?x1,?x3)

SWRL 기반의 추론은 온톨로지의 클래스와 술어로 표현된 원자로 수행되며[13], 선행조건에 지정된 조건이 충족할 때마다 결과에 지정된 조건도 유지되어야 한다. [표 2-5]는 SWRL의 기본규칙 및 규칙을 활용한 예제를 표현한 것으로써 $hasProperty_{1,2,n}$은 추론에 있어 전제 조건에 해당하며 hasFinal은 추론의 결과로 새롭게 생성되며 결론의 역할을 한다. 변수 ?x,?y,?z는 인스턴스 관계 정의에 표현된 개념이나 인스턴스로 대체된다. 따라서 규칙사용의 간단한 예제를 분석하면 부모속성인 Parent는 자신(x1)과 부모님(x2)를 가지고 형제속성인 Brother은 부모님(x2)와 부모님의 형제(x3)속성을 가지므로 자신(x1)과 부모님의 형제(x3)는 삼촌관계가 된다는 의미이다.

C. 지능형 접근제어 기술

1. 접근제어 기술

산업의 발전으로 인한 시스템 안정성 및 제어로부터의 적응 능력에 대한 요구가 커지고 있다. 접근제어(Access Control)란 보안상 위협으로부터 제반 시설 및 환경을 보호하는 보안 대책중 하나이며 정보가 유출되거나 무결성이 훼손되는 것을 방지하기 위해 권한이 주어진 사람에게만 DB에 접근할 수 있도록 통제 및 관리하는 것을 의미한다. 방식으로는 비인가자의 사용을 막는 접근 통제방법인 인증 접근제어와 불필요한 패킷을 걸러내거나 입·출입을 제한하는 패킷 접근제어의 2가지 방식으로 나누어진다.



[그림 2-3] 접근 통제 절차

다음 [그림 2-3]은 접근제어 환경에서의 접근 통제 절차를 간략하게 나타낸 것이다. 보다 자세하게는 정책에 따라 객체의 작업 수행여부를 나타내는 것으로써, 자원에 대한 비인가적 접근을 감시 및 통제한다. 시스템에 접근 요청이 들어오면 요청자를 식별하고, 요청한 방법이 정당한 방법인지를 확인하여 기록한다. 이를 식별이라 한다. 이후 시스템의 패스워드, 토큰, 서명 등 시스템 보안정책에 따라 요청자에 대한 인증 절차를 걸치고, 접근을 승인 혹은 거부함으로써 비인가자에게서의 불법적인 시스템접근 및 파괴를 예방한다[14]. 하지만 실제 시스템의 복잡성, 비선형성 등의 문제로 방대한 전력시스템의 특성상 정확한 모델을 수립하기가 어렵다. 따라서 제어 객체와 제어 규칙을 기반으로 하는 지능적인 방식인 지능형 접근제어 기술을 다음 절에 제시하고자 한다.

2. 지능형 접근제어 기술

[표 2-6] 주요 접근통제 방식 구분

구분	통제 방식
1	사용자 계정관리를 통한 사용자 접근 통제
2	정보 암호화를 통한 접근 통제
3	방화벽 등을 이용한 패킷에 대한 네트워크 접근통제 및 시스템 접근 통제

다음 [표 2-6]은 접근제어 기술에서의 주요 접근통제 방식을 구분한 내용이다.

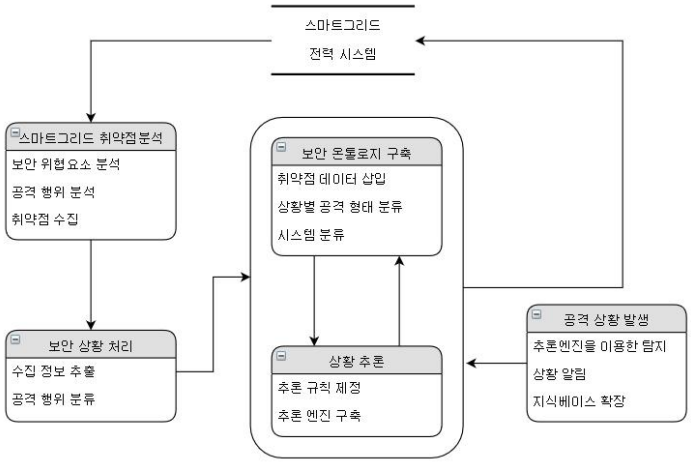
지능형 접근제어란 데이터베이스, 지식 추론, 제어 규칙 등으로 표현됨으로써 통제 규칙의 수립, 그리고 지능형 접근제어 시스템에서의 지식추론 설계로 분류될 수 있다.

지능형 접근제어 시스템의 추론 프로세스는 제어 전략이라 표현할 수 있으며 추론 방법으로는 순방향(정방향)추론, 역추론, 하이브리드 추론 등이 있으며, 본 논문에서는 전력시스템에 발생하는 악성행위에 대해 단계별로 규칙을 적용하는 순방향 추론을 적용해 지능형 접근제어를 하려고 한다. 접근제어 매커니즘은 시도한 접근 요청을 제정한 규칙에 대응시켜 검사함으로써 불법적인 접근을 방어한다[15]. 스마트그리드 전력 시스템에 접근제어 기술을 적용한다면 본 논문에서 사용되는 온톨로지 관련규칙에 관련 내용을 대입하여 보안에 있어 시너지 효과를 낼 수 있을 것이라 전망된다.

Ⅲ. 스마트그리드 보안을 위한 온톨로지 기반 공격탐지 기법

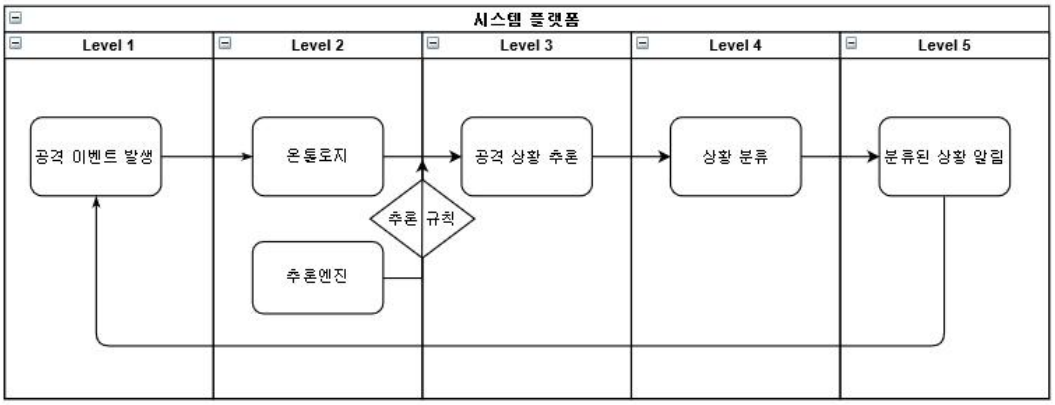
A. 전력 시스템의 보안을 위한 전체 시스템 구성도

공격에 대한 신속한 식별 및 대응이 가능한 지능화된 접근 제어모델을 위해 본 논문에서는 전력시스템에 가해지는 보안 취약점 및 공격 상황을 분석하고, 상황 인식을 위한 온톨로지 구축 및 추론 규칙을 설계하여 전력시스템의 공격 탐지를 위한 방안을 제안한다.



[그림 3-1] 전체 시스템 구성도

[그림 3-1]은 본 논문에서 제안하는 온톨로지를 기반으로 한 전력시스템의 통합 보안 시스템 구성도이다. 시스템의 공격 탐지를 위하여 스마트그리드 전력시스템의 취약점을 수집·분석하고 추출하여 공격 행위를 분류한 후 분석한 데이터들을 기반으로 보안 온톨로지를 구축한 후 제정한 규칙을 통해 상황에 대한 정보를 추론한다. 공격 이벤트값이 발생하면 구축된 온톨로지를 통하여 탐지가 되어 상황을 인식 후 알리며, 발생한 공격 이벤트값의 정보를 추가해 온톨로지의 지식베이스가 확장되게 한다. 실험을 통하여 보안 시스템이 제대로 동작하는지를 확인하도록 한다.



[그림 3-2] 온톨로지 추론과정 프로세스

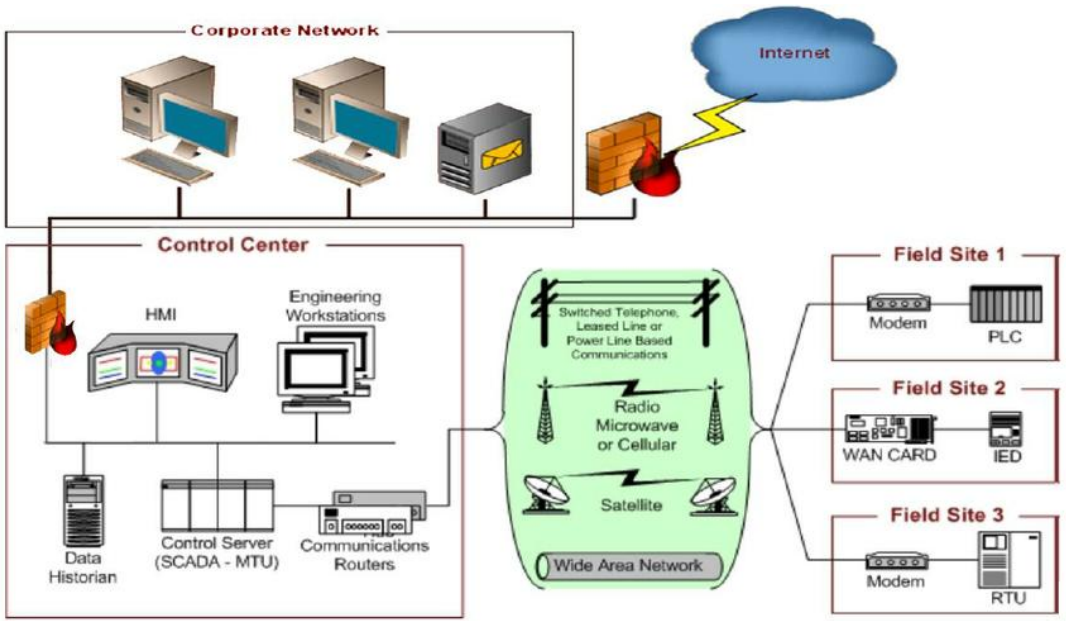
다음 [그림 3-2]는 본문에서 제안하는 전체 시스템 구성도에서 공격 상황이 발생했을 시 온톨로지 추론 과정이 어떠한 단계로 진행되는지를 나타낸 도식도 이다.

구축한 보안 온톨로지 환경에서 Level 1단계의 공격 이벤트 값이 발생하면 Level 2단계의 온톨로지 추론엔진의 제정된 규칙을 통하여 Level 3단계인 공격상황 추론 단계로 넘어가게 된다. 추론을 통해 Level 4단계의 전력 시스템의 어느 클래스에 상황이 발생하였는지를 분류하고, Level 5단계의 분류된 상황을 전파함으로써 전력 시스템의 공격 탐지가 가능할 것이다.

B. 전력 시스템의 보안을 위한 시스템 취약점 분석

전력 시스템의 취약점을 수집 후 분석하여 보안상황을 분류할 수 있다. 전력 시스템은 SCADA(Sypervisory Control and Data Acquisition)시스템을 기반으로 EMS(Energy Management System), MDMS(Meter Data Management System), Metering_System, 등 여러 시스템 및 객체로 구성되어 있다. 각 구성요소가 가지고 있는 영역별 취약점을 전력 시스템 온톨로지에 반영해 공격 탐지를 할 수 있도록 한다.

1. SCADA 시스템의 구조와 보안취약점



[그림 3-3] SCADA 시스템 구성요소

SCADA시스템은 현장기기 및 센서로부터 데이터를 원격단말장치가 수집한 후, 유선,무선 통신망을 통해 중앙제어 컴퓨터에 전송하여 상황을 감시 제어하는 원방감시 제어 시스템이다. 중앙서버, 말단기기, 서버와 기기를 연결하는 통신 네트워크

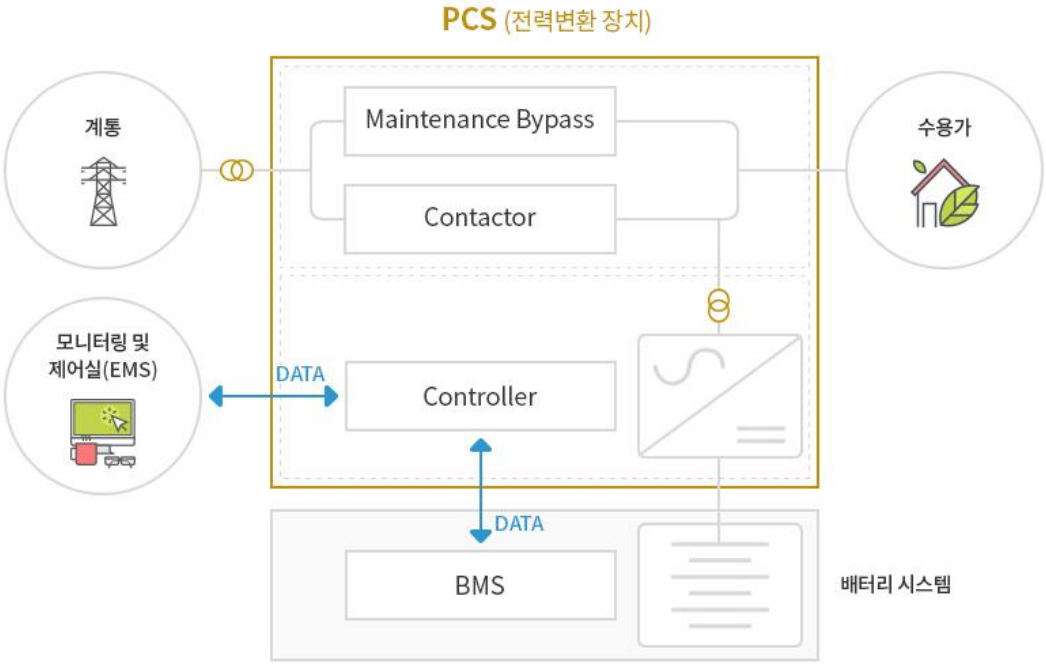
구조로 이루어져 있으며[17], SCADA시스템의 구성요소를 [그림 3-3]으로 나타내었다[18].

[표 3-1] SCADA 시스템의 취약점 분석

공격 방법	내용
통신 데이터 패킷수집 및 분석	SCADA 시스템의 기기들을 연결한 통신선로들에 대한 통신 네트워크에서 발생되는 데이터 패킷을 분석
무선 데이터 패킷 탈취	WAN 무선 통신 과정에서의 데이터 패킷 가로채기
감청	통신 및 무선상의 데이터 정보를 불법으로 분석 및 탈취
위장	탈취한 패킷데이터를 이용하여 정상적 관리자로 위장하여 Control 서버 및 내부 중요데이터에 접근
우회 조작	제어 시스템의 정상적인 동작을 방해하여 공격자가 원하는 방향으로의 불법적 동작을 야기
서비스 지연	서비스 거부공격 등 시스템이 처리할 수 있는 능력을 초과시켜 기능의 지연 또는 마비
Scavenging	관련 시스템의 SW/HW 취약점 조사를 통해 불법적인 접근
바이러스	Trojan, Worm, Backdoor 등 바이러스 공격

SCADA 시스템의 각 구성요소에 발생 가능한 보안 취약점을 분석해 [표 3-1]에 나타내었다. 데이터 패킷 탈취는 통신 네트워크에 발생 가능한 통신데이터 패킷수집 및 분석, WAN 및 Fleld Site의 각 기기별 무선통신 과정중 발생 가능한 무선 데이터 패킷 탈취, SCADA 시스템 전체 구성요소에 발생 가능한 감청으로 구분되며, 이후의 패킷 탈취 후 발생 가능한 제어 센터와 공통 네트워크에 대한 취약점을 정리하였다.

2. EMS 시스템의 구조와 보안취약점



[그림 3-4] EMS 시스템 구성요소

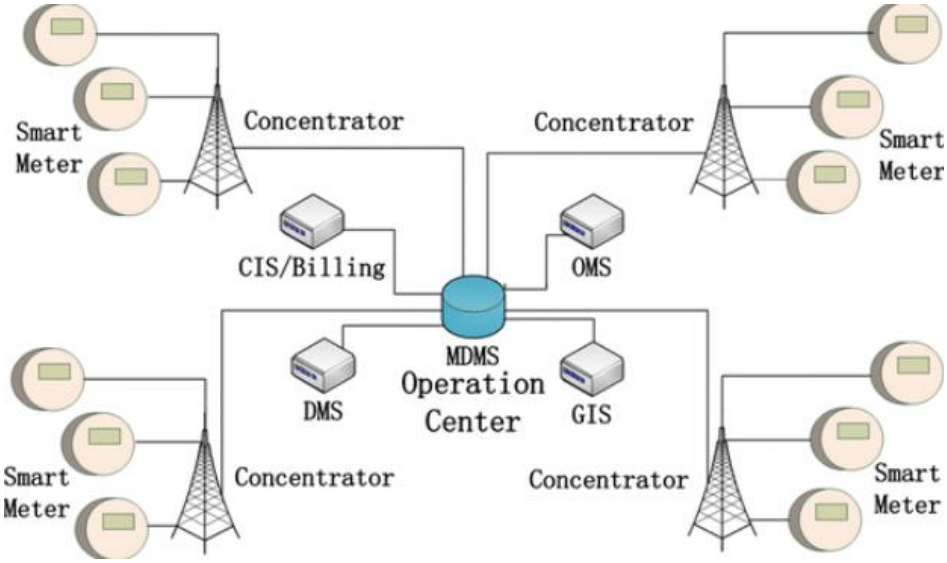
전력시스템 환경에서 에너지 관리를 총괄하는 EMS 시스템은 전력발전량, 전력상태, 전력소비량을 모니터링 하는 시스템으로써, 대규모 미터링 데이터를 실시간 처리하는 역할을 한다. EMS 시스템의 구성 요소를 [그림 3-4]에 나타내었다[19].

EMS 시스템에 주로 발생 가능한 보안취약점은 데이터 수집 단계에서의 미터링 데이터의 조작이며, 공격자의 인위적 행위를 발견하지 못했을 시 위·변조한 에너지 사용정보로 인해 에너지 저장 시스템에 문제가 발생할 수 있기 때문에 각별히 주의하여야 한다. 또한 에너지 사용 정보 수집 시스템의 취약점을 통해 전력 소비자의 전력거래 금액 조작 및 개인정보의 유출의 문제점이 제기된다. 관련된 보안 취약점을 정리하여 [표 3-2]에 나타내었다.

[표 3-2] EMS 시스템의 취약점 분석

공격 방법	내용
서비스 거부 공격	스마트 미터, 게이트웨이 등을 대상으로 하여 시스템 동작의 지연 또는 마비
메시지 변조	통신기기간 전달되는 메시지 변조를 통한 기기 오작동 유발
바이러스	관련 시스템의 업데이트에 악성 바이러스를 삽입해 시스템 오작동 및 파괴
데이터 스니핑	통신 프로토콜의 스니핑을 통한 데이터 위변조
물리적 공격	건물에 설치된 정상 기기를 해체 후 악성 바이러스에 감염된 기기로 교체
펌웨어 조작	기기의 펌웨어를 조작해 손상시켜 오작동 유발
감청	IP 망을 통한 시스템 원격제어 시 사용자의 정보를 빼내어 정보 유출 및 위변조

3. MDMS 시스템의 구조와 보안취약점



[그림 3-5] MDMS 시스템 구성요소

실시간 통신하며 소비자의 전력 사용정보를 보관하며, 소비자 미터기에 명령을 내려 다양한 정보를 관리하는 MDMS 시스템은 전용망 네트워크로 구성되어 있으며 관련 구성요소를 [그림 3-5]에 표현하였다[20].

전용망 네트워크의 구성 특성상 외부에서의 직접적인 공격이 제한되지만, 내부로부터의 취약점 공격에는 취약하다는 단점이 있다. 대중적으로 널리 알려진 스턱스넷이나 두쿠와 같은 악성 바이러스를 USB같은 저장매체를 이용하여 내부망을 통해 감염 및 빠르게 전파시켜 관련 시스템에 큰 악영향을 끼치거나 소비자가 전력사용정보를 보기 위해 스마트 미터와 연동된 앱 및 웹서비스, 서버의 취약점을 이용한 공격행위를 가진다. MDMS 시스템에 관련된 취약점을 정리하여 [표 3-3]에 나타내었다.

[표 3-3] MDMS 시스템 취약점 분석

공격 방법	내용
웹 서비스 취약점 공격	사용자 관리를 위한 웹 서비스의 취약점을 이용한 불법접근
앱서비스 취약점 공격	스마트 미터 기기와 연동된 앱을 통해 불법적으로 접근한 후 내부 데이터 수집
서버 취약점 공격	DB서버에 접근하여 계량정보를 확인 후 위변조 행위
바이러스	저장매체를 통한 악성 바이러스 감염
스푸핑	감염 기기를 정상 장비로 인식하여 주변 스마트미터 기기로 전송

4. Smart Meter 시스템의 보안취약점

전력시스템의 구성 도메인들을 토대로 취약점을 분석해본 결과 전체적인 전력시스템을 표현하기는 많은 제약점이 있기에 본 절에서는 전력 시스템을 구성하고 있는 시스템중 하나를 예시로 들어 공격 탐지를 위한 온톨로지의 구축 시나리오를 전개하고자 한다.

예시로 표현한 스마트 미터 시스템은 전력을 이용하는 가정 및 빌딩에 설치하여 전력 소비자에게 가격, 신호, 사용량 등 실시간 정보를 알려줌으로써 에너지 절약을 유도하는 전력시스템 구성요소이다. 관련된 공격 툴킷 및 취약점 정보가 다양해 공격자의 악성행위가 나타나는 빈발지수가 높고, 공격의 난이도도 어렵지 않기 때문에 적용하였으며, 온톨로지의 구축에 앞서 스마트 미터에 가해지는 공격 행위 및 취약점을 정리하였다.

[표 3-4] 스마트 미터에 가해지는 공격 행위[16]

공격 방법	내용
변조 공격	전력정보를 가로채 전력 사용량을 변경시켜 올바른 검침이 되지 않도록 방해함.
프라이버시 공격	도청이나 트래픽 분석을 통해 소비자의 전력 사용량을 파악해 에너지 소비정보 악용
물리적 공격	스마트 미터 내에 부채널공격(Side Channel Attack)을 이용해 직접적으로 접근하여 데이터를 변경하거나 유출시킴
침투 공격	웜,바이어스, 트로이 목마와 같은 악성 코드를 스마트 미터에 침투시키며 전산망 침투의 가능성이 있다.
서비스 거부공격	스마트 미터가 처리할 수 있는 능력을 초과토록 해 자원을 고갈시켜 기능을 마비시킴
불법 도용 공격	중간자 공격과 재사용 공격을 통해 전력 정보를 도청 혹은 변경할 수 있음.
운영 시스템 공격	시스템 자체의 취약점을 이용하여, 스마트 미터의 허가권과 명령권을 얻을 수 있음.

[표 3-5] 스마트 미터 취약점 분석

취약점 종류	내용
불법 접근	홈 게이트웨이와 연결된 인접 네트워크를 통한 접근
원격 접근	Zigbee 통신 등 보안위험성이 있는 통신 프로토콜 사용
물리적 공격	보안이 갖춰져 있지 않은 스마트 미터의 회로 및 침입하기 쉬운 암호 알고리즘
평문 전송	양방향 통신으로 인한 암호화 되지 않은 상태로의 정보 전송
키 관리 미흡	공개키 구조
시스템의 부재	낮은 보안성의 인증정책 및 백업, 복구에 대한 시스템의 부재
악성행위 탐지	서비스 거부공격 및 바이러스 침투에 대한 탐지능력 부족

[표 3-6] 스마트 미터 취약점 세부 분석[8]

상세 정보	설명
버스 스니핑	스니핑을 통한 환경정보, 암호화 키 추출
펌웨어 취약점 공격	바이너리 소스코드 분석을 통한 버퍼 오버플로우, 취약점 추출
다이 분석	물리적으로 단말기에 침입해 데이터 내용을 읽고 상태정보 추출
템퍼링 보호기술 공격	낮은 보안성의 템퍼링 보호기술 공격
컨트롤 시스템 위장	인가되지 않은 사용자가 컨트롤 시스템 역할을 하며 미터기 조작, 펌웨어 불법 업데이트 등 악성행위 수행
전자기 간섭	전기신호를 통해 기기의 암호연산 및 처리능력 파악
메모리 덤프	메모리 덤프를 통한 사용자의 정보 추출

다음 [표 3-4]은 스마트 미터에 가해지는 공격 행위에 대한 분류를 나타낸 것이다. 방법은 각각 변조 공격, 프라이버시 공격, 물리적 공격, 침투 공격, 서비스 거부 공격, 불법 도용 공격, 운영시스템 공격의 7가지로 분류할 수 있다[21]. 분류한 공격 행위 데이터를 기반으로 스마트 미터의 취약점을 분석해 [표 3-5]와 [표 3-6]에 나타내었다.

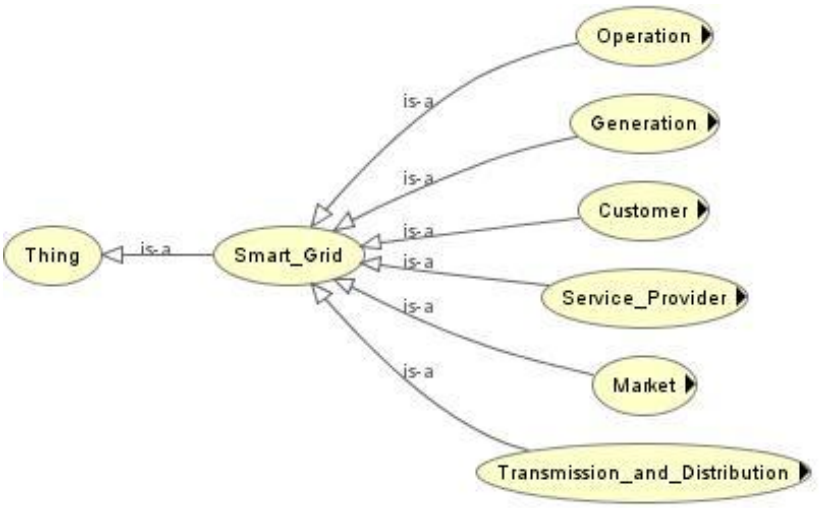
공격을 수행하기 전 공격자들은 관련 취약점을 먼저 분석하고, 취약점을 바탕으로 공격 행위가 발생하기 때문에 스마트미터에서 분석된 취약점을 나타낸 [표 3-5]와 [표 3-6]을 바탕으로 시스템을 구축한다.

여러 가지의 모의해킹 사례를 분석해 보았을 때[18] 장비의 취약점을 파고들어 인접한 광역 시스템에 쉽게 접근해 국가적으로 큰 피해를 입힐 수 있는 중요한 장비이며 따라서 이를 빠르게 인식할 수 있는 시스템이 필요하다.

C. 공격 탐지를 위한 온톨로지 구축 및 추론규칙 설계

1. 전력시스템 온톨로지 구축

스마트그리드를 구성하는 시스템들은 송전부터 시작해 전력소비를 하는 고객에 이르기까지 여러 종류의 시스템으로 구성되어 있다[18]. 따라서 전력시스템 온톨로지를 구축하기 위해 관련 시스템들을 토대로 클래스 개념을 통해 구성한다.



[그림 3-6] 기본 클래스 관계도

[그림 3-6]은 본 실험에 앞서 전력시스템 온톨로지의 구성을 위해 7개의 관련 도메인을 모델화 하여 나타낸 것이다. 기존의 스마트그리드 국가 로드맵에서는 5개의 도메인(소비자, 전력망, 서비스, 신재생, 운송)으로 하위 클래스를 제정하였으나, 본 논문에서는 보다 나은 상황 인식을 위하여 세분화한 모델을 제시하였다. 송전 및 배전 클래스의 경우 이들을 구성하는 하위 클래스가 동일하기 때문에 통합하여 표현 하였다. 이후 관련 클래스의 하위 클래스를 정의하여 논문에서 제안하는 전력시스템 구축과정을 살펴보기로 한다.

[표 3-7] Level 2와 Level 3클래스 정의

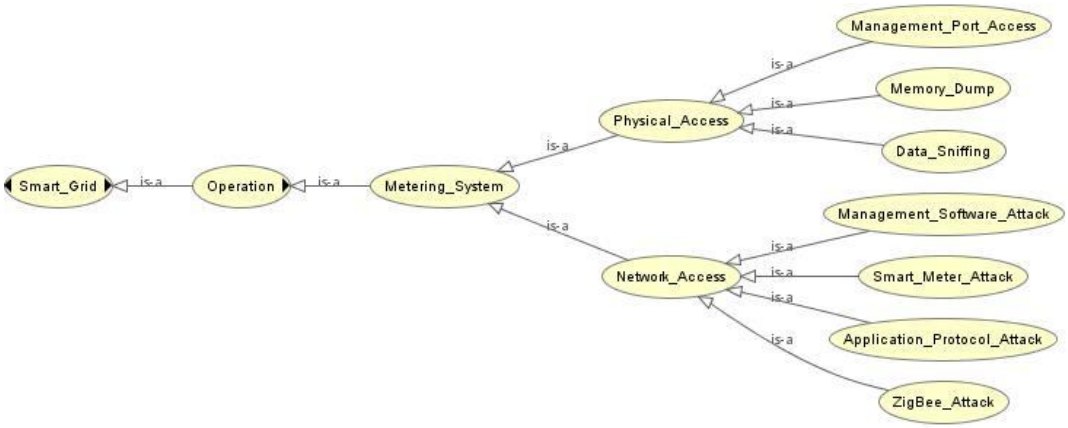
Level	Class	Level	Class
2	Operation	3	Asset_Management
			EMS
			Metering_System
			DMS
			MDMS
			Distribution_SCADA
			WAMPAC
			Demand_Response
			Transmission_SCADA
2	Generation	3	Generator
			Electric_Storage
			Market_Service_Interface
			Plant_Control_System
2	Customer	3	Energy_Service_INterface
			Customer_Equipment
			Thermostat
			Customer_EMS
			Appliances
			Meter
			Customer_Substation
2	Service_ Provider	3	Home_Manager
			aggregator
			Retail_Energy_Provider
			CIS
			Billing
			Others
2	Market	3	Retailer
			Energy_Market_Clearinghouse
			Aggregator
2	Transmission_ and_ Distribution	3	Data_Collector
			Field_Device
			Substation_Controller
			Substation_Device

[그림 3-7] 전력 시스템 온톨로지 관계도

전력시스템 온톨로지를 구축하여 [그림 3-7]에 나타내었고, 관련 구성요소를 [표 3-7]에 나타내었다. 구축한 전력시스템 온톨로지는 총 Level 5 단계의 클래스로 구성되어 있지만 각 클래스를 전부 기입하기엔 지면상 제약사항이 따르므로 핵심 시스템인 Operation 클래스의 하위 클래스 Metering System을 예로 들어 표현한다.

[표 3-8] Level 3부터 Level 5까지의 클래스 정의

Level	Clasee	Level	Class	Level	Class
3	Metering _ System	4	Network _Access	5	Application_Protocol_Attack
					Smart_Meter_Attack
					Management_Software_Attack
					ZigBee_Attack
		4	Physical _Access	5	Management_Port_Access
					Memory_Dump
					Data_Sniffing



[그림 3-8] Metering System 관계도

Level 3단계의 Metering System 클래스의 하위 클래스를 각각 [표 3-8]과 [그림 3-8]로 표현하였다. Metering System에 접근하는 방법을 크게 Level 4단계의 물리적 접근과 네트워크적 접근의 2단계로 분류하였으며, 가해지는 공격행위를 Level 5 단계로 세부분류 하였다. 온톨로지 분류를 세분화 할수록 공격상황이 발생하였을 때에 어느 시스템에서 공격이 발생했는지를 판별하는데 파악하기가 쉽기 때문에 관련 상황별 온톨로지 분류는 매우 중요한 요소라고 할 수 있다.

2. 전력시스템 온톨로지 속성 정의

앞 절에서는 클래스와 레벨값들을 정의하였다면 본 절에서는 클래스의 속성을 정의한다.

[표 3-9] 주요 Property 정의

Class	Property	설명
Total	resultIn	해당 행위에 대한 결과값
	behavior	나타나는 행위값
	hasType	행위에 대한 종류
	hasEffect	행위의 효과
	hasPurpose	행위에 대한 공격 목적
Network_Access	usedConfig	이벤트 등록
	usedFileread	장치 목록 조회
	usedFilewrite	장치 파일 제어
	hasRemoteControl	장치 원격 제어
	hasProtocol	장치 프로토콜 값
	hasRegistrationDate	행위정보의 발생 일자
Physical_Access	isLocated	미터링 시스템의 위치
	hasUserId	사용자의 아이디
	hasPassword	사용자의 암호
	has_Key	사용자의 키값
	hasLocalControl	장치 로컬제어
	hasRegistrationDate	행위정보의 발생 일자

[표 3-9]는 Metering_System 클래스의 주요 Propery의 정의를 나타낸 것으로써, 전체 클래스와 네트워크 접근, 물리적 접근의 세 분류를 통해 앞서 표현하지 못했던 클래스의 데이터 속성값을 정의하였다.

3. 공격 탐지를 위한 추론규칙 설계

온톨로지 설계 이후 추론규칙 제정은 상황을 인지하고 분석하는데 있어서 매우 중요한 작업이다. 전력시스템에 가해지는 공격은 앞에서 분류한 여러가지 시스템의 취약점에 접근해 타겟에 대한 공격을 실시하게 된다. 따라서 본 절에서는 취약점을 이용한 공격행위를 단계별 상황 분류를 통해 SWRL 언어로 추론규칙을 설계하였다.

잘 알려진 스마트미터 시스템의 취약점을 이용한 공격 상황 정보를 기반으로 물리적 접근과 네트워크 접근에 대한 취약점 추론규칙을 [표 3-10]과 같이 정의하였다.

[표 3-10] 물리적·네트워크적 공격단계 추론규칙

situation	Rules
Physical_Access	(?T Memory_Readout_Techniques) ∧ (Memory_Readout_Techniques resultIn Memory_Reading) ∧ (Memory_Reading resultIn Data_Gathering) => (?T Side_Channel_Attack)
Network_Access	(T? behaviour Data_Sniffing)∧(Data_Sniffing resultIn Packet_Decoding)∧(Packet_Decoding resultIn Key_Acquisition)∧(Key_Acquisition resultIn Data_Gathering) ⇒ (?T step Data_Sniffing)

공격단계는 공격자가 직접적으로 시스템 공격을 하기 전 관련 정보를 획득하는 단계이다. 물리적 접근방식과 네트워크 접근방식의 두가지 방식으로 행위를 나타내었다. 추론규칙에서 물리적 접근방식의 경우 외부에 비치된 스마트 미터나 관련 회선에 직접적으로 침투하여 같은 트랜잭션을 여러번 반복수행한 후 메모리를 읽고 정보를 획득하게 된다. 이를 이용하여 스마트미터 내부의 전력에 데이터 등을 획득할 수 있게 된다. 네트워크적 공격단계에서는 데이터 스니핑을 통해 각 패킷을 디코딩하여 내용을 분석해 스마트미터 기기상의 암호키 및 인증서를 획득할 수 있게 된다. 획득한 키를 이용해 시스템에 접근한다. [표 3-11]은 시스템 접근단계에서의 추론규칙을 나타낸다.

[표 3-11] 시스템 접근단계 추론규칙

situation	Rules
System_Acess	(?T behaviour Key_Acquisition)∧(Key_Acquisition resultIn Data_Gathering)∧(Data_Gathering resultIn System_Access) => (?T Back_Door)

공격단계에서 관련 사용자 암호키 및 인증서를 획득하고 분석하면 공격자는 취약점을 이용해 시스템에 접근하게 된다. 이 단계를 본 논문에서는 시스템 접근단계라고 정의한다. 접근방식을 나눈 본절의 [표 3-10]과는 다르게 같은 상황으로 가정했으며 이는 물리적인 취약점을 이용해 접근한 공격자도 시스템을 공격하려면 같은 상황에 봉착하기 때문이다. 시스템 접근단계에서는 획득한 키 및 사용자 정보를 이용해 접속하게 되며 접속 후 악의적인 행동을 위해 백도어를 삽입하여 공격을 할 수 있는 통로를 제공하게 된다.

[표 3-12] 시스템 조작단계 추론규칙

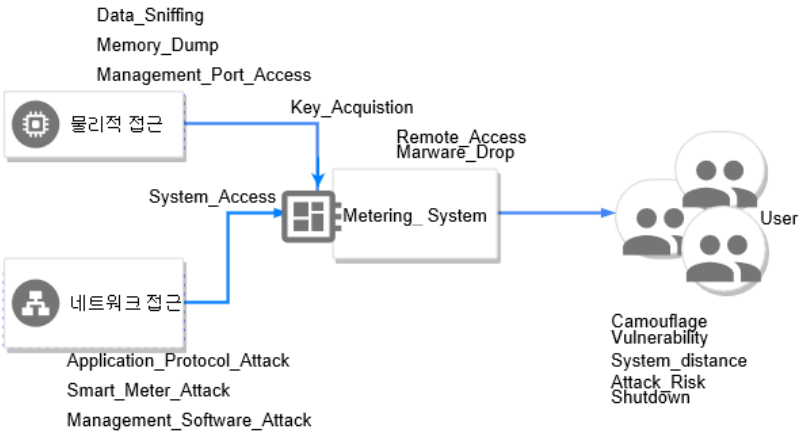
situation	Rules
Remote_Access	(?T behaviour Data_Gathering)∧(Data_Gathering resultIn System_Access)∧(System_Access resultIn System_Control) => (?T REMOTE ACCESS)

[표 3-12]은 스마트미터 시스템에 접근한 공격자가 미터기 시스템의 정보를 불법적으로 조작할 수 있는 시스템 조작 단계이다. 이 단계에서는 전력제어 시스템을 이용해 시스템을 공격하거나, 조작된 전력데이터 사용량을 사용자에게 보낼 수 있으며, 잘 알려진 스턱스넷이나 두쿠와 같이 전력시스템을 마비시킬 수 있는 환경을 제공해 주는 단계이다[22].

이밖에도 여러 가지 공격상황 규칙을 제정하였으나, 가장 빈번하게 발생하는 상황정보를 간추려서 추론규칙을 표현하였다.

[표 3-13] 온톨로지를 통한 객체간 관계 표현

구분	내용	예시
객체	온톨로지를 활용한 인지 개체 정보	Management_Software_Attack, Management_Port_Access, Memory_Dump, Data_Sniffing, ...
객체간 관계	객체간 관계 정보	Attack_Risk, System_distance, Vulnerability, Camouflage, ...
상황	추론된 상황 정보	Marware_Drop, System_Access, Remote_Access, Key_Acquistion, Data_Gathering, ...



[그림 3-9] 상황추론 진행 과정

[표 3-13]는 온톨로지를 통한 객체간 관계 예시를 표현한 것이다. 스마트미터에 발생되는 공격을 클래스화 시킨 것으로써 상황이 일치하는지를 판별하고, 추론된 관계들은 다음 시점에 추론하는 관계와 연계된다.

[그림 3-9]는 단계별로 규칙을 적용하는 순방향 추론에 따라 어떠한 방식으로 추론이 진행되는지를 나타낸 것으로써 상황이 발생하면 어떠한 방식으로 추론이 되는지를 표현하였다.

Ⅳ. 실험 및 평가

A. 공격 상황 시나리오 구성

본 장에서는 제안하는 스마트그리드 전력시스템의 공격 탐지를 위한 온톨로지 구축 시스템의 성능 측정을 하고자 앞서 제안했던 스마트 미터에 가해지는 공격 상황을 시나리오로 구성하여 나타내었다.

[표 4-1] 상황 시나리오

내용
전력시스템의 보안업무를 맡고 있는 'A'씨는 금요일 저녁 퇴근 전 스마트 미터를 설치한 가정에서 설치된 스마트 미터가 갑자기 동작 장애가 발생되었다는 민원을 받았다. 퇴근시간이 얼마 남지않아 간단하게 확인 해본 결과 별다른 특이사항이 일어나지 않아 특이사항 없음이라고 보고하고 퇴근한 'A'씨는 일요일 저녁 인근의 스마트미터 시스템이 전부 멈추었다는 긴급호출을 받고 급하게 회사로 출근했다. 출근해서 상황을 확인해본 결과 퇴근 전 민원이 발생한 스마트 미터 단말기에서 인접한 다른 단말기에 전력망을 통하여 악성코드를 전파한 상황을 확인할 수 있었고, 확인한 시점에도 계속하여 다른 단말기로 악성코드는 계속 전파되고 있었다. 보안상황을 고려해 스마트미터는 보안이 인증된 기기를 사용하며, 보안 관제팀이 시스템 상황을 확인하고 있었음에도 불구하고 악성코드가 손쓸 새도 없이 전파된 상황.

스마트 미터 보안상황중 가장 일반적으로 발생하는 상황을 가정하여 본 장에서는 [표 4-1]에 상황 시나리오를 가정하여 보았다. 스마트 미터 단말 시스템에서 갑작스러운 원인불명의 시스템 동작 장애가 일어난 상황에서 'A'씨는 상황을 간단하게만 확인하였으며, 이는 인근의 다른 단말기에 시스템 셧다운이라는 큰 피해를 입히게 되었다.

스마트그리드 전력시스템 환경은 양방향 통신을 이용하기 때문에 네트워크 공격에 큰 피해를 입을 수 있기 때문에 이러한 상황에서는 시스템의 취약점을 이용한 공격임을 의심하고 신속하게 관련 환경을 점검했어야 한다.

B. 시나리오 정보에 기반한 공격 상황 추출

본 절에서는 앞서 언급한 공격상황 시나리오 정보에서 관련 상황 정보를 추출하여 나타내었다.

[표 4-2] 공격상황 추출 및 클래스 정의

순서	공격 상황	Class
1	패킷 탈취 후 시스템 접근	System_Access
2	민원인 가정에서의 스마트 미터 동작장애	DDoS_Attack, ExIPPacketSize
3	인접 단말기 바이러스 전파 및 감염	Various_Attack, Various_Infection
4	인근의 스마트 미터 시스템들의 동작 정지	System_Shutdown

[표 4-2]는 상황 시나리오에서 발생한 공격 상황들을 단계별로 분류하고 서브 클래스를 표현하였다.

첫 번째 공격 상황인 패킷 탈취 후 시스템 접근 상황은 상황 시나리오에 표현되있지는 않았으나 공격을 위해서는 물리·네트워크적 접근을 통한 패킷을 탈취하여야 시스템에 접근할 수 있기 때문에 순서 1로 가정하였으며, 이후의 공격 상황은 상황 시나리오대로 표현된다.

두 번째 공격 상황인 민원인 가정에서의 스마트 미터 동작 장애 상황은 공격자가 시스템에 접근했는지 확인하기 위한 상황으로써 DDoS 공격을 통한 시스템의 자원을 부족하게 하거나 의도적으로 용량이 큰 패킷을 계속해서 보내 시스템의 동작 장애를 일으키는 상황이다.

세 번째 공격 상황인 인접 단말기 바이러스 전파 및 감염 상황은 공격자가 두 번째 공격 상황에서 시스템에 성공적으로 접근하였다면 원래 목표했던 대로 바이러스를 인접 단말기에 전파하고 악성행위를 하는 상황이다. 추가적으로 백도어를 삽입해 시스템에 계속 접근할 수 있는 통로를 만들 수도 있는 상황이다.

네 번째 공격 상황인 인근의 스마트 미터 시스템들의 동작 정지 상황은 가장 최악의 시나리오로써, 셧다운 제어명령을 내려 감염된 시스템들의 대량 정전을 일으키는 상황이다.

공격 상황에서는 평균적으로 세 번째 상황까지 일어나며 네 번째 상황은 드물게 일어나지만, 본 논문에서 제안한 전력 시스템에 일어나는 공격 탐지를 위해서는 최상위 공격 단계까지 설계해야하기 때문에 이에 대한 관련 상황 및 클래스를 표현하였다.

C. 시나리오 정보에 기반한 공격 상황 탐지

시나리오에 기반한 공격상황을 추출한 후 SWRL언어로 작성된 각 단계별 설계 규칙을 통하여 공격 상황 탐지 추론식을 [표 4-3]과 같이 나타내었다.

[표 4-3] 공격 상황 탐지 추론식

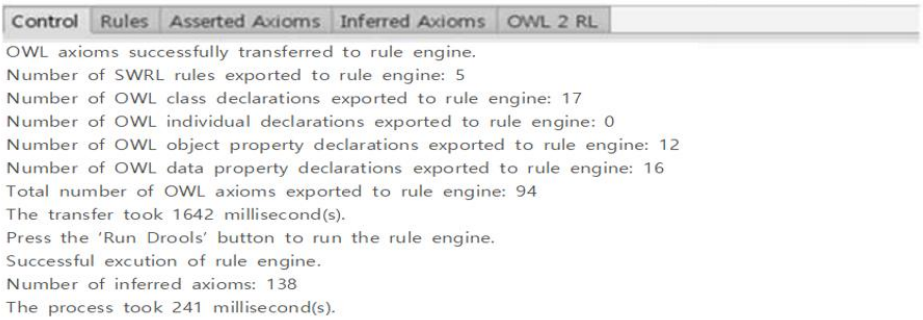
situation	Rules
Network_Access	(T? behaviour Data_Sniffing)∧(Data_Sniffing resultIn Packet_Decoding)∧(Packet_Decoding resultIn Key_Acquisition)∧(Key_Acquisition resultIn Data_Gathering) ⇒ (?T step Data_Sniffing)
System_Access	(?T behaviour Key_Acquisition)∧(Key_Acquisition resultIn Data_Gathering)∧(Data_Gathering resultIn System_Access) => (?T Back_Door)
Remote_Access	(?T behaviour Data_Gathering)∧(Data_Gathering resultIn System_Access)∧(System_Access resultIn System_Control) => (?T REMOTE ACCESS)
Movement	(?T behaviour Back_Door)∧(Back_Door resultIn Adjacent_System)∧(Adjacent_System resultIn Malware_Drop) => (?T Various_Attack)
ShutDown	(?T behaviour Various_Attack)∧(Various_Attack resultIn System_Access)∧(System_Access resultIn System_Control)∧(System_Control resultIn Destruction) => (?T System_Shutdown)

네트워크 접근부터 시작해 시스템 접근, 시스템 조작, 악성 바이러스의 시스템간 이동, 시스템 셧다운까지의 공격 전개과정을 도출하였다. 작성한 추론식을 실행하여 추론식이 실제로 실행되는지를 확인한다.

[표 4-4] 시스템 구현 환경

개발 도구	Protégé 4.3 Version
사용 언어	OWL(Web Ontology Langauge)
운영체제	Windows 10 Education 64bit
HW 사양	Intel Core i5-4570 3.2GHz Memory 4GB SSD 1TB

스마트그리드 전력 시스템의 보안을 위한 시스템 구현 환경은 다음 [표 4-4]와 같다. 개발 도구는 Protégé 4.3 Version을 사용하였으며, 언어 및 추론 엔진은 Protégé에 내장되어 있는 엔진을 사용하였다. 운영체제는 Windows 10 64bit를 사용하였다.



[그림 4-1] SWRL 추론식 실행 결과

온톨로지 추론 엔진에서 SWRL기반 추론식을 실행한 결과 [그림 4-1]의 결과값이 나오는 것을 확인하였으며, 성공적으로 실행되는지를 하단에서 3번째 Successful excution of rule engine의 문장을 통해 확인할 수 있었다.

전력 시스템에 가해지는 여러 가지 공격 시나리오와 상황정보들에 대해 제정한 추론규칙을 이용하여 실행결과의 추론규칙값 실행여부를 통한 결과를 아래 [표 4-5]에 나타내었다.

[표 4-5] 상황별 추론 인식 여부

공격 패턴	공격 상황 정보 및 추론규칙	실행 여부
Memory Dump	공격자의 메모리 덤프를 액세스를 통한 정보탈취 및 시스템 손상	○
	(?T behaviour Memory_Dump_Access)∧(Memory_Dump_Access resultIn usedFileread)∧(usedFileread resultIn Buffer_Overflow)∧(Buffer_Overflow resultIn Key_Acquisition)∧(Key_Acquisition resultIn System_Damaged)	
Port Access	네트워크 키 및 계량정보 등 중요정보 추출	○
	(?T behaviour Port_Access)∧(Port_Access resultIn Routing_Attack)∧(Routing_Attack resultIn Session_Hijacking)∧(Session_Hijacking resultIn Meter_Data)	
Data Sniffing	사용자의 정보를 빼내고 암호화 키 정보의 추출	○
	(T? behaviour Data_Sniffing)∧(Data_Sniffing resultIn Packet_Decoding)∧(Packet_Decoding resultIn Key_Acquisition)∧(Key_Acquisition resultIn Data_Gathering)	
Software Attack	펌웨어 취약점을 공격하여 악성펌웨어 업데이트	○
	(?T behaviour Firmware_Attack)∧(Firmware_Attack resultIn usedConfig)∧(usedConfig resultIn File_Update)	
Protocol Attack	관련 패킷을 추출한 후 재전송을 통한 공격	○
	(?T behaviour Intercept_Packet)∧(Intercept_Packet resultIn extraction_Packet)∧(extraction_Packet resultIn Relay_Message)	
ZigBee Attack	보안 네트워크 발견 및 장치 식별 공격, 패킷 차단 공격	○
	(?T behaviour Network_Access)∧(Network_Access resultIn Traffic_Capture)∧(Traffic_Capture resultIn Traffic_Save)	

시스템에 발생 가능한 여러 가지 상황 패턴별 시나리오를 준비하고, 추론규칙을 세워 구축한 전력시스템 보안 온톨로지가 정상적으로 동작하는지를 확인해 보았다. 추론 규칙의 실행여부는 확인할 수 있었지만, 방대한 스마트그리드 시스템에 대한 공격방법은 매우 다양하기 때문에 확률적인 통계치를 나타내는 것에 대해서는 어려움이 있다고 판단된다. 따라서 본 논문에서 제정한 규칙들을 조합해 추론 규칙의 복잡성을 늘려야 할 것이다.

V. 결론 및 제언

본 논문은 스마트그리드 전력 시스템에 가해지는 공격 취약점을 분석하고 이에 따른 공격 행위 분류를 통해 공격 탐지를 위한 지능형 접근제어 온톨로지를 구축하였다. 온톨로지를 구축하기 위해 스마트그리드 도메인의 정보를 토대로 관련 시스템들을 나열하였으며, 주요 도메인의 시스템별 공격 취약점들을 분석하고, 취약점을 이용한 공격 상황에 대한 상황인지 모델링에 초점을 두었다. 또한 공격이 발생하는 형태 및 순방향 추론기법을 이용해 네트워크 접근 시스템 접근, 시스템 조작, 악성 바이러스의 시스템간 이동, 시스템 셧다운의 공격 순서에 따른 구축법을 적용하였다.

논문에서의 실험은 전력 시스템에의 핵심기기인 스마트 미터를 예로 들어 가장 일반적으로 발생할 수 있는 공격 상황을 가정해 시나리오를 작성해 보았으며, 스마트 미터 시스템의 취약점을 이용한 단계별 공격경로를 확인하는 추론규칙을 작성하고, 추론식을 실행해 결과를 확인할 수 있었다. 이후 다른 공격 시나리오들의 추론규칙 실행 여부를 통하여 구축된 온톨로지를 평가하였다.

적용한 온톨로지 시스템은 효율적인 규칙 적용을 통해 대용량의 온톨로지 처리에 유리한 이점을 지니고 있어 지식베이스 구축에 있어서 온톨로지의 유연한 시스템은 데이터의 최신성 유지 및 데이터의 유용성, 확장성, 위협분석 정보 활용에 큰 장점이 될 수 있음을 나타낸다.

향후 연구로는 스마트그리드 전력 시스템을 구성하는 시스템들의 잘 알려지지 않은 취약점을 분석해 공격행위에 따른 추론 규칙의 수정 및 추가를 통해 온톨로지 추론 규칙의 복잡성을 늘려 더욱 다양한 보안 상황을 인식하고, 신속한 대응을 하는 것을 목표로 한다.

참고문헌

[1] 유성민, 김남균, 김윤기. “스마트그리드 보안기술 동향분석 및 대응방안”, 한국통신학회지(정보와통신), Vol.31, No.5, pp.8-14, 2014.

[2] https://www.unsw.adfa.edu.au/school-of-engineering-and-information-technology/identifying-smart-grid-vulnerabilities-due-cyber-attacks

[3] 산업통상자원부. “스마트미터기·에너지저장장치 보급방향”, 2013.

[4] 이건희, 서정택, 이철원. “스마트그리드 사이버 보안 추진 현황”, 정보보호학회지, Vol.20, No.5, pp.7-13, 2010.

[5] 전효정, 김태성. “AMI 공격 시나리오에 기반한 스마트그리드 보안피해비용 산정 사례”, 정보보호학회논문지, Vol.26, No.3, pp.809-820, 2016.

[6] 한국방송통신전파진흥원. “스마트그리드 구축을 위한 AMI기술동향”, 방송통신기술 이슈&전망, Vol.53, 2014.

[7] 김태식, 강동주. “전력시스템의 사이버보안 위협 규명 및 분류에 대한 연구”, 보안공학연구논문지, Vol.9, No.2, pp.53-65, 2012.

[8] 에너지경제연구원. “안전한 스마트그리드 구축 및 활용을 위한 법제도 개선방안”, 지식경제부, 2012.

[9] 최승훈. “시맨틱 웹 기술을 이용한 확장된 특성 모델의 제한조건 검증”, 한국정보기술학회논문지 Vol.9, No.10, pp.229-236, 2011.

[10] M. Uschold, M. Gruninger, “Ontologies : principles, methods and applications″, Knowledge Engineering Review, Vol.11, No.2, pp.93-136, 1996.

[11] http://obitko.com/tutorials/ontologies-semantic-web/semantic-web-architecture.html

[12] 이승우, 정한민, 김평, 서동민. “추론기술연구동향”, 주간기술동향 통권, No.1446, pp.1-12, 2010.

[13] 이완곤, 방성형, 박영택. “분산처리 환경에서 SWRL 규칙을 이용한 대용량 점증적 추론 방법”, 정보과학회논문지, Vol.44, No.4, pp.383-391, 2017.

[14] 이범기, 김미선, 서재현. “IoT에서 Capability 토큰 기반 접근제어 시스템 설계 및 구현”, 정보보호학회논문지, Vol.25, No.2, pp.439-448, 2015.

[15] Shukun Cao, Xiangbo Ze, Jing Xu, Lei Shi. “Intelligent Control System of Multi-segments Continuously Sintering Furnace”, DOI: 10.1109/KAM.2008.183, 2008.

[16] 정철조, 은선기, 최진호, 오수현, 김환구. “스마트미터의 취약성/보안요구사항 분석 및 CC v3.1 기반 보호프로파일 개발”, 정보보호학회논문지, Vol.20, No.6, pp.111-125, 2010.

[17] 강동주, 이종주, 이영, 이임섭, 김휘강. “전력 SCADA 시스템의 사이버 보안 위험 평가를 위한 정량적 방법론에 관한 연구”, 정보보호학회논문지, Vol.23, No.3, pp.445-457, 2013.

[18] Abdelghafar M. Elhady, Ahmed Abou Elfetouh S, Hazem M El-Bakry, A. E. Hassan. “Generic Software Risk Management Framework for SCADA System”, International Journal of Computer Applications, Vol.70, No.3, pp.45-52, 2013.

[19] http://www.scec.co.kr/sub/smartgrid/ess.php

[20] Su Ma, Hong Zhang, Xiaomin Xing. “Scalability for Smart Infrastructure System in Smart Grid: A Survey”, Wireless Personal Communications, Vol.99, No.1, pp.161-184, 2018.

[21] NIST, “Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0”, 2010.

[22] 서정택, “스마트그리드 보안위협 및 대응전략”, 대한전기학회 스마트그리드연구회 춘계학술대회, pp.17-57, 2013.

저작물 이용 허락서

학 과	소프트웨어융합공학과	학 번	20178422	과 정	석사
성 명	한글: 김기훈 한문 : 金起勳 영문 : Kim Gi Hoom				
주 소	전라남도 순천시 신대로 96, 중흥 S클래스 307동 202호				
연락처	E-MAIL : kkh20114672@gmail.com				
논문제목	한글 : 스마트그리드 환경에서 보안을 위한 온톨로지 기반 공격탐지 기법 영문 : Ontology-based Attack Detection for Security in Smart Grid Environments				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함
2. 위의 목적을 위하여 필요한 범위 내에서의 편집·형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 또는 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물의 이용허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음
7. 소속대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의(√) 반대( )

2018년 12월 27일

저작자: 김 기 훈 ()

조선대학교 총장 귀하