2018년 8월

석사학위 논문

스마트그리드 환경에서 지능형 접근제어 서비스를 위한 보안 상황인식

조선대학교 산업기술융합대학원

소프트웨어융합공학과

김 태 양

2018년 8월

석사학위논문

스마트그리드 환경에서 지능형 접근제어 서비스를 위한 보안 상황인식

김 태 양

스마트그리드 환경에서 지능형 접근제어 서비스를 위한 보안 상황인식

Security Context Awareness
for Intelligent Access Control Service in Smart Grid

2018년 8월 24일

조선대학교 산업기술융합대학원

소프트웨어융합공학과

김 태 양

스마트그리드 환경에서 지능형 접근제어 서비스를 위한 보안 상황인식

지도교수 최 준 호

이 논문을 공학석사학위신청 논문으로 제출함.

2018년 4월

조선대학교 산업기술융합대학원

소프트웨어융합공학과

김 태 양

김태양의 석사학위논문을 인준함

위원장 조선대학교 교수 반 싱 법 (인)

위 원 조선대학교 교수 신 주 현 (인)

위 원 조선대학교 교수 최 준 호 (인)

2018년 5월

조선대학교 산업기술융합대학원

목 차

표 목 차

그 림 목 차

ABSTRACT

Security Context Awareness for Intelligent Access Control Service in Smart Grid

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

With the depletion of energy sources and the rising demand for electric power around the world, a concept called a smart grid has emerged to address challenges such as preventing global warming and reducing carbon emissions. The smart grid is an intelligent power technology developed by integrating ICT technology with existing power grid that is centralized and unidirectional with 'generation-transmission-distribution-supply' steps. It is a technology that induces consumers to voluntarily save energy and optimizes energy efficiency by enabling suppliers and consumers to exchange real-time energy usage information in a bidirectional way. Various latest ICT technologies such as Advanced Metering Infrastructure (AMI), IoT, Home Network Area (HAN), cloud computing, etc., are being integrated for the smart grid.

With various smart grid technologies being developed and extended, various new security threats that did not occur in an existing environment can occur. With the use of bidirectional communication technology for interconnections between power systems and component equipment, targets of attack and threats are increased. System information and vulnerabilities are exposed to the outside due to the increased use of commercial hardware and software. Since there are numerous contact points between consumer sections and smart grid systems and is equipment physically distributed in a wide area, it is difficult to manage them and also various intrusion paths are allowed for attackers.

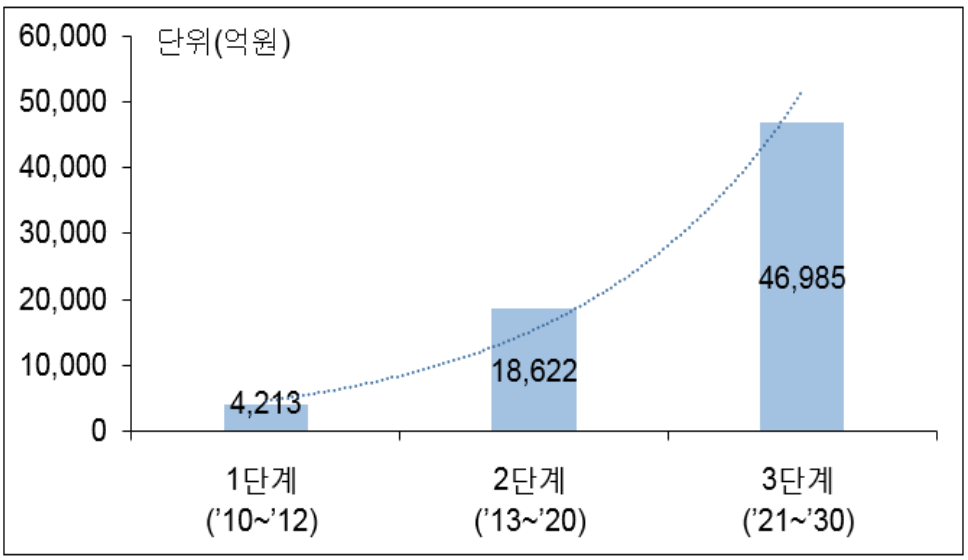
Since an attack on a power system can cause extensive damage at the national level, integrated and intelligent security technologies are required as a countermeasure against various and intelligent attacks. Security intrusion detection and countermeasure technologies for conventional power systems generally use pattern-based and behavior-based statistical methods. However, they cannot be a fundamental solution to increasingly intelligent and diversified security attacks.

In this paper, we first built a situation information ontology model based on security situation information of power systems in a smart grid environment with the aim of recognizing security situation for smart grid intelligent access control service. We then designed an intelligent security situation recognition model that can respond quickly by using security weakness of power systems and an inference engine, and proposed a method that can be applied in major power systems.

Ⅰ. 서론

A. 연구 배경 및 목적

전 세계적으로 전력수요가 증가하여 에너지원의 고갈되고 있고 지구 온난화 방지 및 탄소 배출량 감소와 같은 과제를 해결하기 위해 스마트그리드라는 개념이 발생하였다. 나라별로 전략적 추진 성격이 조금씩 다르다. 미국은 노후화된 전력계통의 고도화, 유럽은 신재생 에너지의 활용 활성화, 일본은 효율적인 에너지 관리 등을 목표로 스마트그리드 기술을 추진하고 있다[1]. 우리나라는 에너지사용에 대한 비용감소와 신재생에너지기술을 발전 및 확대하여 수출 산업화와 국제 경쟁력을 확보하기 위해 스마트그리드 기술을 도입하고 있으며 국가발전의 새로운 패러다임으로 “저탄소 녹색성장”의 비전과 구체적 실행방안으로 국가 단위 스마트그리드를 2030년까지 구축할 계획을 제시하였다[2]. [그림 1-1]은 우리나라에서 스마트그리드 핵심 기술개발을 위한 투자 계획을 그래프로 표현하였다[3].



[그림 1-1] 스마트그리드 기술개발 투자 계획

스마트그리드에 사용되는 기술은 AMI(Advanced Metering Infrastructure)와 IoT 기술, 클라우드 컴퓨팅과 스마트 미터 기술 등의 다양한 최신 ICT 기술이 접목되고 있다[4][5]. 이로 인해 기존 환경에서는 방생하지 않았던 새로운 보안위협이 발생할 수 있다. 기계 장비가 커넥티드 환경에서 진행되기 때문에 시스템 간의 외부 연결이 필수가 되었고 무선통신의 보안 취약점을 악용한 공격이 가능해졌다. 스마트그리드 기술의 개발과 발전이 증가하면서 이처럼 다양한 사이버 공격에 노출될 것으로 예상한다. 공격이 전력시스템에 가해지면 기존 정보통신 분야의 피해 규모보다 방대한 국가적인 피해를 유발할 가능성이 있다[6][7]. 스마트그리드를 대상으로 하는 공격 방법이 다양해지고, 지능화되는 추세로 이에 대한 대응책으로 통합적이고, 지능적인 보안기술이 필요하다.

전력시스템에서의 기존 보안 침해사고 탐지 및 대응 기술은 일반적으로 패턴 기반과 행위 기반 등의 통계적인 방법이 주로 사용되었는데, 이는 갈수록 지능화, 다형성 성격을 갖는 보안 침해 공격에 대한 근본적인 해결책이 될 수 없다. 따라서 현재 지능형 시스템에서 연구가 활발히 진행되고 있는 온톨로지 기술, 시맨틱 웹 기술에 기반을 둔 다양한 추론 기술, 지능형 접근 제어모델, 텍스트 마이닝과 자연어 처리기술에 기반을 둔 악성 코드 탐지 기술 등 전력시스템에서의 보안 침해사고에 대해 다양한 지능형 추론 기술을 도입하여 지능적으로 보안 침해사고에 대응할 수 있고, 온톨로지 추론을 이용한 접근 제어기술을 이용한 효과적인 대응 방법이 필요하다.

B. 연구 내용 및 구성

본 연구는 스마트그리드 환경에서 전력시스템의 보안상황 정보를 기반으로 상황 정보 온톨로지를 모델링하고 전력시스템의 보안취약점과 추론 엔진을 이용하여 신속한 대응이 가능한 지능화된 상황인지 접근 제어 모델을 설계하고 주요 전력시스템에서 적용할 수 있는 방안을 제시하고자 한다. 이를 제안하기 위해 다음과 같이 구성한다.

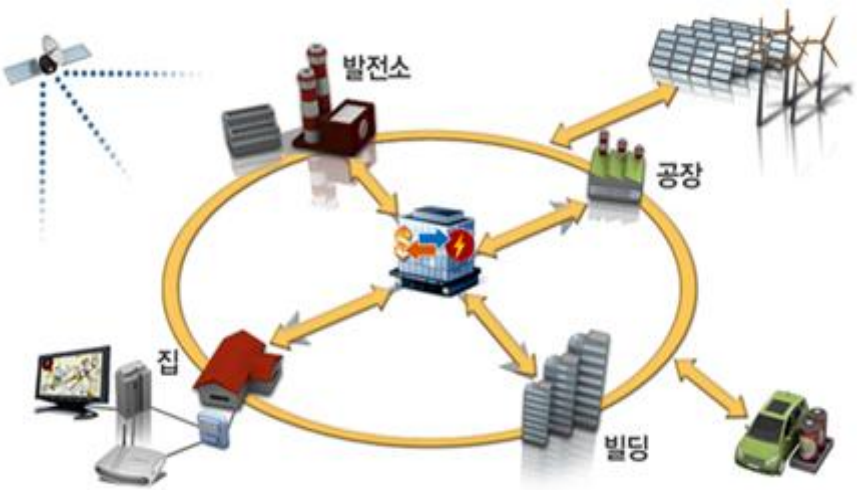
서론에서 연구배경의 목적과 필요성에 관해 설명하고 2장 관련 연구에서는 연구의 이론적인 배경으로 스마트그리드의 보안 현황과 침해사례 및 기존 연구들을 설명하고 보안 상황인식에 대해 간략히 설명한다. 3장은 논문에서 제안하는 온톨로지 기반의 지능형 접근제어 서비스 설계를 위해 전력시스템의 취약점들을 수집하고 분석을 통한 온톨로지 설계에 관하여 설명한다. 4장에서 실험환경과 실험에 사용한 추론규칙 설계에 관해 설명하고, 테스트 실험을 통해 추론식을 확인한다. 마지막으로 5장에서 결론과 향후 연구에 관해 서술하며 마무리한다.

Ⅱ. 관련 연구

A. 스마트그리드 보안현황

1. 스마트그리드 보안 취약점 및 침해사례

스마트그리드는 단일화된 '발전-송전-배전-판매' 단계로 중앙 집중적인 운영인 기존 전력망에 ICT 기술을 융합하여 발전시킨 지능형 전력기술로 전력의 공급자와 소비자 사이에서 실시간 에너지 사용정보를 양방향으로 전달해주며 소비자의 자발적인 에너지 절약을 유도하며 에너지 효율을 최적화 시켜주는 기술이다[8].



[그림 2-1] 스마트그리드 개념 (출처:스마트그리드사업단)

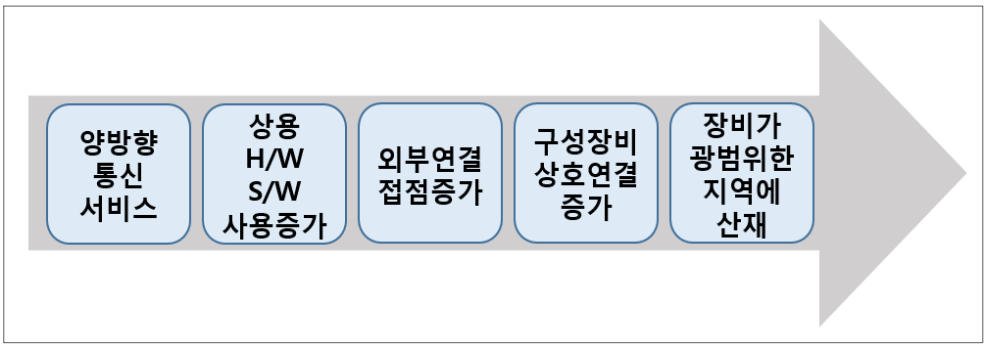
[그림 2-1]은 스마트그리드 사업단에서 정리한 스마트그리드 개념을 표현하는 그림이다[]. 발전소의 전력생산과 스마트 팩토리, 스마트 빌딩, 스마트 홈 등을 통한 실시간, 양방향적인 통신으로 전력효율을 최대화한다. 스마트그리드는 나라별, 기관별로 조금씩 정의가 다르지만 큰 맥락에서의 의미는 비슷하다. 아래 [표 2-1]은 스마트그리드 정의에 대하여 정리한 표이다[9, 10, 11].

[표 2-1] 스마트그리드 정의

나라 / 기관	정의
미국	에너지 독립 및 안보법에서 미래에 증가할 에너지 수요를 완화시키고 전력 전송과 분배에서 신뢰성 있고 기반시설 보호를 유지하도록 구조화된 지능형 국가전력 전송 분배 시스템
유럽	지속 가능하고 효율적인 안전한 전기 공급의 전송을 위하여 연결된 모든 관계자 및 이용자들의 행위를 지능적으로 통합할 수 있는 네트워크
스마트그리트 협회	기존 전력망에 ICT기술을 적용하여 전력생산, 소비정보를 양방향, 실시간 교환하여 에너지 효율 최적화 목적의 차세대 전력망
스마트그리드 사업단	기존의 전력망에 최신의 정보통신기술을 이용하여 공급자와 수요자 사이에 실시간 정보를 양방향으로 교환하면서 지능형 수요관리와 신재생 에너지 연계 등이 가능한 차세대 전력인프라 시스템
위키백과	전기의 생산부터 운반과 소비 과정에서 정보통신기술을 사용하여 공급자와 소비자가 상호작용함으로써 효율성을 높인 지능형 전력망 시스템

스마트그리드는 전력생산자가 통제하는 수직적, 중앙 집중적인 네트워크가 아닌 수요자와 공급자 간에 상호작용을 가능하게 해주는 수평적, 분산적 네트워크를 구축함으로써 에너지의 효율적인 이용과 에너지 설비투자 절감 효과, 그리고 신재생에너지 확대 및 기후변화 대응을 기대할 수 있다. 또한 전기사용 형태 및 전기 요금 정보의 실시간 제공으로 소비자의 자발적 에너지 절약을 유도하고 요금이 낮은 시간대의 전기수요를 유도하여 전력수요를 분산할 수도 있는 장점이 있다.

스마트그리드에서 전력 효율 최적화와 같은 장점이 생길 수 있는 가장 큰 요소는 양방향 통신이다. 하지만 스마트 미터와 같이 전력 공급자와 수요자 사이의 양방향 통신을 위한 연결통로가 생성되면서 전력시스템에 대한 사이버 보안위협도 같이 증가한다. [그림 2-2]는 이러한 스마트 그리드에 대한 사이버 공격을 가능하게 해주는 보안위협 요소들이다[12]. 스마트그리드에 연결된 수천만 개의 스마트 미터기를 이용한 DDoS 공격 형태의 대규모 공격이 발생할 수 있으며 스마트 그리드의 기능이 마비되게 된다.



[그림 2-2] 스마트그리드 보안 위협요소

양방향 통신기술을 사용하게 되면서 보안위협이 증가하였다. 스마트그리드는 스마트 미터기와 전력공급업체, 관리업체 사이에 양방향 통신을 사용하기 때문에 데이터 위·변조 공격을 당하면 전력계통 운영 방해와 과금정보 조작을 통해 금전적인 피해가 발생할 수 있다. 상용 하드웨어와 소프트웨어 사용 증가로 인해 시스템정보와 취약점이 외부에 노출되는 등 기존 전력망에 비해 사이버 공격에 대한 보안위협 증가하였다. 전력 소비자 입장에서 시스템으로 수많은 접점이 많아지는데 수천만대의 스마트 미터와 전기차 등이 전력망에 연결되며 스마트그리드 시스템으로 접근 가능한 지점이 대폭 증가하게 되면서 보안위협이 증가하였다. 스마트그리드 기기 간 상호연결 증가로 인해 지능화된 서비스 제공을 위하여 기존의 통신 구조에서 주변의 스마트그리드 기기와 통신을 수행하는 등 상호연결성 증가로 위험관리가 어려워졌고 광범위한 지역에 분산된 스마트그리드 장비 사용으로 스마트 미터, 배전 센서 등의 스마트그리드 장비가 광범위한 지역에 물리적으로 산재하여 위험관리 및 보안관제가 어렵다.

[표 2-2] 스마트그리드 환경에서 보안 침해 공격 형태

공격 형태	설명
신분 위장	합법적 신원을 이용하여 불법적 통신을 시도하는 공격으로 침입자는 스마트 미터의 신원을 가장하여 전력 소비 비용을 지불할 수 있음.
도청	스마트그리드 환경에서 객체 및 장치들이 통신하는 동안 교환되는 데이터에 대한 접근이 가능하여 특정 가정의 에너지 소비를 쉽게 도청할 수 있음.
데이터 손상	전력사용 데이터를 수정하여 적은 전력 요금 시간으로 수정하는 공격이 가능하고 전력 과소비를 초래하여 과부하 발생이 가능함.
권한 부여 및 접근 제어	스마트 미터 혹은 배전변전소에 설치된 센서와 같은 장치들이 원격으로 구성되어 감시당할 수 있고 공격자는 불법적 접근을 조작하여 변압기의 정전을 유발할 수 있음.
악성 코드	스마트그리드의 객체는 원격에서 물리적으로 침해의 대상이 될 수 있음. 센서와 같은 제약적인 물리적 장치들은 손쉬운 침해 대상이 될 수 있음.
가용성 및 DDoS 공격	스마트그리드 환경의 전력 장치는 프로토콜 기반 가용성 및 DDoS 공격의 대상이 될 수 있음.
물리적 자산 공격	스턱스넷(Stuxnet)과 같은 사이버 공격은 스마트 미터와 변압기, 케이블 등의 물리적 자산을 위태롭게 할 수 있음.

위의 [표 2-2]는 스마트그리드 환경에서 보안 침해 공격 형태를 정리한 표이다. 이외에도 수많은 보안 침해공격이 가능하며 실제 보안침해 공격 사례들을 정리하였다. 에너지 분야와 관련된 사이버 공격은 2000년 이후로 나타나기 시작했다. 원자력 발전소와 같은 사회기반시설에 대한 공격이 발생하며 엄청난 규모의 피해와 사회적으로 큰 혼란을 야기할 수 있음을 입증하였고 정부와 기관에서의 보안에 대한 관심이 높아졌다. 스마트그리드 기술은 미래 에너지 산업분야의 하나이므로 과거 사회기반시설 및 산업제어시스템 등에 관한 보안 침해 사건을 연구하여 사이버

위협으로부터 시스템을 보호할 수 있도록 대비하여야 한다. [표 2-3]는 스마트그리드 관련 보안 침해 사건이다[13][14].

[표 2-3] 스마트그리드 관련 보안 침해 사건

연도	발생 국가	보안침해 내용
2015	우크라이나	피브치나 변전소 해킹으로 인한 정전
2014	한국	사회기반시설 공격 목적의 kimsuky 악성코드
2014	유럽	SCADA 프로그램 하벡스 악성코드
2014	일본	몬주원전 해킹으로 내부자료 유출
2012	블랙햇	스마트 미터와 AMI 취약점에 관한 공격방법
2010	이란	스턱스넷을 이용한 원자력발전소 공격
2009	CNN	스마트미터 취약점을 이용해 운영센터 침입확인
2009	푸에토리코	스마트미터관련 직원의 해킹으로 전력량 조작
2007	에스토니아	DDos공격으로 국가시스템 3주간 마비
2003	미국	원자력 발전소의 제어망으로 슬래머웜 침투

[표 2-3]와 같이 에너지 분야의 사이버공격은 2000년 이후로 지금까지 지속적으로 발전해왔고 공격방법 또한 더 다양해졌다. 가장 빈번하게 발생하는 위협으로는 2003년 원자력발전소를 공격한 슬래머 웜부터 2010년 이란 핵시설을 공격한 스턱스넷과 이후 꾸준히 발전 변종된 악성코드들의 감염에 의한 사건이다. 관리자의 미숙과 윤리문제로 인한 내부자의 의한 공격도 있으며 기관 및 기업 대상의 모의해킹 침투에 의한 사건 등을 통해 앞으로의 공격가능성을 확인하였다. 스마트그리드 환경에서의 가장 염려되는 공격위협은 AMI 시스템에서의 공격으로 실시간, 양방향적인 통신을 위하여 불가피하게 공개된 네트워크망을 사용하여야 하고 스마트미터와 같은 전자장비와 이를 이용한 무선 통신 구간에서의 취약점이 확인되었다.

스마트그리드에서 개인정보 유출, 정전사태 등 공격의 종류가 다양해지고, 공격의 수준이 높아지고 있음. 전력 공급의 중추인 스마트그리드 환경에서의 사이버 공격은 국가 전력 마비와 같은 심각한 피해를 주게 됨. 스마트그리드를 대상으로 하는 공격 방법이 다양해지고, 지능화되는 추세로 이에 대한 대응책으로 통합적이고, 지능적인 보안기술이 필요하다. 위에서 언급한 보안 취약점들을 연관지어 전력시스템에서 발생하는 다양한 보안침해사고에 대한 명확한 판단과 신속한 대응을 위해 보안상황 온톨로지를 설계하고, 이를 기반으로 추론규칙과 제약조건을 정의한 후, 이를 전력시스템에 실제 적용할 수 있는 연구가 필요하다.

2. 스마트그리드 보안관련 연구

스마트그리드보안 관련 기존 연구들은 크게 기술적 연구와 정책적 연구로 나누어진다. 스마트그리드를 구성하는 주요 전력시스템별로 연구하여 인증을 위한 새로운 프로토콜 및 암호화 기법을 사용하거나 기존 시스템의 통신프로토콜 개선과 같은 기술적 연구등이 있다. 정부 및 기관에서 발표한 스마트그리드보안 관련 보고서나 동향기반의 연구논문들은 스마트그리드 보안을 위하여 법과 제도의 개선과 같은 정책적 의미의 연구들이 많다.

[표 2-4] 스마트그리드 보안관련 연구

연구 분야	관련 연구 논문
기술 연구	스마트그리드기반 스마트홈에서의 서비스거부공격 대응기법
	적시성 향상을 위한 PUSH방식 AMI시스템 성능비교
	전력IT 제어시스템에 대한 사이버공격 대응방안을 위한 연구
	스마트그리드의 AMI를 위한 ETDTP설계
	지능형검침인프라(AMI)사이버보안 위험분석
	스마트그리드지능형소비자를위한 보안프레임워크 개발
정책 연구	마이크로그리드 환경의 전력망 보안위협 정량적 평가방안 연구
	보안위협사례 분석을 통한 전력제어시스템 보안평가항목
	국내 법 규정 및 표준에 적합한 한전 AMI시스템 보안정책에 관한 연구
	스마트그리드 서비스에서의 개인정보보호를 위한 기술적 관리적 방안마련 및 시범적용
	클라우드 기반 스마트그리드를 위한 보안기술 연구

스마트그리드 보안관련 연구들은 스마트그리드를 구성하는 하나의 전력시스템에서 보안을 위한 프레임워크의 제안이나 복잡한 형태의 통신 프로토콜을 제안하는 등 기술적인 연구부터 스마트그리드의 전체 취약점을 개선하기 위해 취약점, 위험을 평가하는 항목을 제안하거나 법과 제도 등을 개선하여 스마트그리드 보안을 높이려는 연구까지 매우 다양하다. 기술적인 연구들은 스마트그리드 전체적인 기술적 요소를 제안하기에 어려움이 있고 각 항목들 간에 보안을 높이는 반면 지능화된 프로토콜 및 기기들을 이용하기에는 국가적 규모에서 적용하기엔 한계가 있다.

B. 보안 상황인식

1. 온톨로지와 추론

온톨로지는 특정 도메인 내 지식을 개념화(Conceptualization)하고, 이를 명세화(Specification)하는 것으로 특정 분야의 지식체계를 컴퓨터가 해석하고 이해하여 처리할 수 있도록 형식화한 표준 명세서이다. 어휘 사전의 역할과 함께 지식을 효과적으로 표현하고, 메타데이터에서 사용되는 클래스, 속성 등의 정보를 계층적으로 표현하며, 정보의 의미를 부여하고, 정보 간의 관계를 설정할 수 있다. 또 광범위한 도메인에 적용할 수 있도록 표준을 제시하며 웹 문서에 나타난 지식을 표현하고 재사용과 공유를 목적으로 하고 있다. [표 2-5]은 온톨로지의 구성요소를 정리하였다[15].

[표 2-5] 온톨로지의 구성요소

구성요소	세부 설명
개념	일반적인 사물 혹은 개념에 붙이는 본질적인 인식이나 지식
인스턴스	사물이나 개념의 구체물이나 사건 등의 형태로 나타낸 각 Class의 실례
속성	Class나 Instance의 개념에 근본적으로 속해 있는 성질
관계	Class, Instance 간에 존재하는 관계 (is-A, has-A)

온톨로지는 컴퓨터와 사람 사이에서 정보 공유와 재사용을 위한 시맨틱 웹의 핵심으로 컴퓨터가 정보의 의미를 이해하고 사람에게 제공할 수 있도록 데이터와 정보, 지식 등의 개념과 관계를 표현하는 형식으로 개념 간 연결을 통해 표현하며, 연결 관계에 대한 추론을 통해 정의되지 않았던 새로운 개념적 관계 추론할 수 있다. 추론은 이미 알고 있는 명제를 기반으로 논리적 결론을 도출하기 위한 행위 또는 과정을 말하며 온톨로지에서의 추론은 온톨로지에 명시적으로 표현된 사실에서 암묵적으로 내제된 사실을 이끌어내는 과정이다. 추론 방법으로는 크게 2가지가 있는데 기술 논리 기반의 추론과 규칙 기반의 추론 기법이 있다. 기술 논리기반의 추

론기법은 추론결과에 대한 정확성과 완전성이 보장되지만 대용량 온톨로지에 대한 추론에 있어 효율성이 떨어진다. 규칙기반 추론기법은 효율적인 규칙 적용을 통해 대용량의 온톨로지 처리에 유리하다[16]. 온톨로지에서 추론을 위한 언어로 SWRL(Semantic Web Rule Language)을 사용하였는데 관계추론을 위한 규칙을 정의할 수 있다.

[표 2-6] SWRL 기본규칙

SWRL 기본규칙
$hasProperty_1(?x, ?y) \wedge hasProperty_2(?y, ?z) \wedge .... hasProperty_n(?y, ?z) \Rightarrow hasFinal(?x, ?z)$

$hasProperty_1()$과 $hasProperty_2()$, $hasProperty_n()$은 앞의 역할 및 속성을 정의하기 위해 기술된 표현으로 추론에 있어 전제 조건에 해당한다. hasFinal은 추론의 결과로 새롭게 생성되는 관계이며 결론의 역할을 제공한다. 변수 ?x, ?y, ?z는 개념, 인스턴스 관계 정의에 표현된 개념이나 인스턴스로 대체된다. 이와 같이 일반화된 표현은 다시 특정 도메인에서 요구하는 규칙에 적합하게 변경될 수 있다[]. 전제와 결과는 A1 ∧...∧An 으로 쓰인 원소들의 AND 결합으로 변수들은 접두사로 물음표를 붙이는 기본 협약에 의해 나타낸다[17].

[표 2-7] SWRL 규칙 예

SWRL 규칙 예
$hasPizza(?x, ?y) \wedge hasSameCheeze(?y, ?z) \Rightarrow hasUse(?x, ?z)$

“피자는 도우(x)와 모짜렐라치즈(y)를 갖고, 모짜렐라치즈(y)와 체다치즈(z)가 둘 다 치즈라면 도우(x)는 체다치즈(z)를 사용할 수 있다.” 고 표현되는 문장은 Pizza와 SameCheeze 프로퍼티들의 조합을 전제로 두고 Use 프로퍼티를 결과로 나타낼 수 있으며 [표 2-7]의 규칙 예와 같이 정의된다. ?x, ?y, ?z 등은 변수를 나타내고 각 변수명 앞의 hasPizza, hasSameCheeze, hasUse는 속성을 의미한다.

2. 상황인식 추론

사용자와 관련 있는 정보 및 서비스를 사용자에게 제공하는 과정에서 상황을 사용하는 경우 상황인식 시스템이라고 말할 수 있다. 사용자 중심의 지능화된 서비스를 제공하는 기술상황 인식, 상황의 특징을 추출하고 학습하며 추론하는 등의 지능화된 기법을 사용하여 인간 중심적인 자율적인 서비스가 가능하다. 상황의 범주와 분류는 정의되는 방식에 따라 달라질 수 있지만 거의 모든 정보는 상황정보로 분류될 수 있으며 특정 상황에 관련된 객체가 지정되면 상황정보 추출이 가능하다. 상황인지 기술은 주변 상황을 인식하여 시스템이 스스로 상태를 변경하거나 사용자에게 필요한 서비스를 제공하는 것을 말하고 센서를 통한 좁은 의미의 상황인지 기술부터 빅데이터를 활용한 인공지능의 개념까지 광범위한 의미를 가지고 있다. 상황인식을 이용한 서비스들이 이루어지기 위해서는 적절한 상황정보의 수집, 처리, 그리고 정보에 따른 판단이 이루어져야 하는데 이를 위해 상황 모델링, 상황인지, 추론 엔진, 서비스관리 등의 기술이 필요하다.

상황이 무엇인지 정의가 내려진 이후에는 정보들을 어떤 방식으로 수집 및 가공하고 어디에서 불러오고 어디로 전달할 지를 결정하는 상황 모델링과 정보모델을 바탕으로 상황정보를 모으는 과정인 상황 센싱은 주로 여러 소스로부터 상황정보를 수집하고 이들 정보를 모델에 따라서 내부에 저장하는 과정을 거치며 추론을 위한 기초자료가 된다. 상황정보를 수집하면 데이터를 융합하여 상위 상황정보를 유도할 수 있는데 상황정보 기반의 지능적인 추론 방법을 제공하여야 실제 애플리케이션에서 유용한 정보로 활용할 수 있게 된다[18].

상황인식은 규칙을 가지고 그 행동을 하게 되는데 상황판단은 추론규칙으로부터 도메인별로 상황을 통해 패턴화되고 관계를 적용하면 상황인식에 따라 행동하기 때문에 상황을 판단할 수 있다. 센싱기술과 인공지능 기술의 발달로 점차 인지 가능한 상황의 범위가 넓어지며 환경 조정, 개인 정보, 감정과 같은 부분까지 다양한 분야에 적용을 기대할 수 있다. 상황인식시스템에서 상황모델의 표현능력을 증가시키고 정형화된 모델표현 방법을 사용하며 사용의 편리성과 적용성을 제공하기 위해 온톨로지 기반 상황모델을 사용한다.

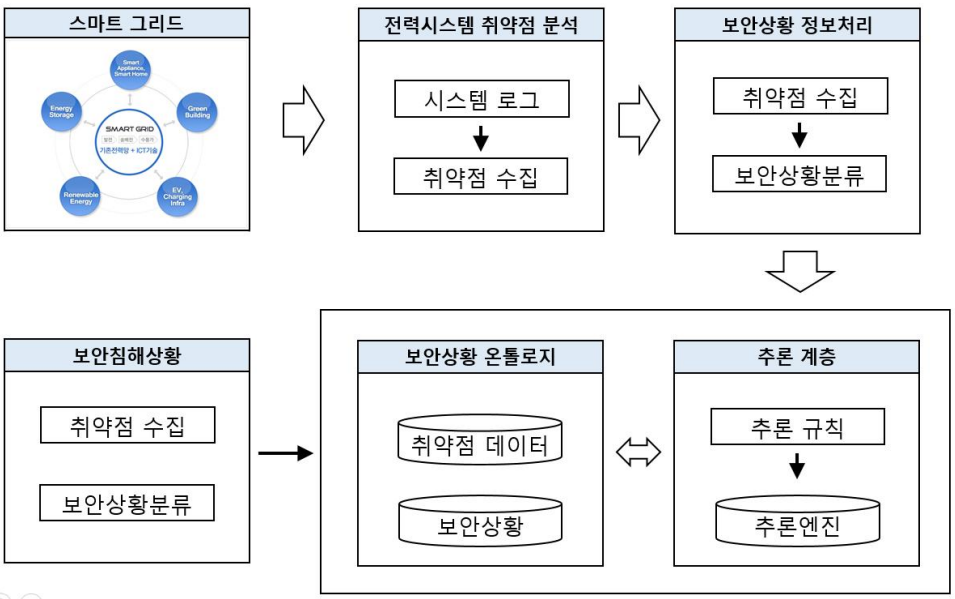
상황모델은 상황인식을 위해 물리적인 환경 개념의 종류와 조건, 관례 등이 명시적으로 기술되어야하며 기계가 읽을 수 있는 규격으로 표현되어야 한다. 여러 유형의 상황모델이 있지만 온토로지 기반 상황모델은 다른 모델들에서 표현할 수 없었던 복합적인 상황 데이터를 표현할 수 있다. 추론을 위한 도구로 상황 시나리오를 통해 서술한 관계집합에 대한 일관성을 점검할 수 있으며 기본 상황 데이터에서 인스턴스 집합과 관계를 통해 보다 추상적인 상황 묘사를 나타낼 수 있다.

기존에 연구된 대표적인 온톨로지 기반의 상황모델은 CoBrA와 CONON이 있다[19][20]. CoBrA(Context Broker Architecture)는 스마트공간에서 상황 인식 시스템을 지원하기위한 에이전트 기반 아키텍처로 'EasyMeeting'이라는 지능형 회의실 시스템을 프로토타입으로 만들어 설명하였고 회의에서는 Context Broker가 온톨로지 및 논리 추론 규칙을 사용하였다. CONON는 퍼베이시브 컴퓨팅 환경에서 컨텍스트를 모델링하기 위한 확장 가능을 목적으로 제안된 상황모델로 상위 수준 엔티티 집합을 모델링하고 다양한 응용 프로그램 도메인에 특정 개념을 추가 할 수 있는 확장성에 대한 유연함을 제공한다. 상황인식은 논리적인 추론 메커니즘을 사용하였는데 설명 논리를 이용하는 온톨로지 추론과 1차 논리를 이용한 사용자 정의 추론으로 분류하였다. 두 연구 모두 스마트 공간(회사, 홈)에서 사람과 장소, 센서 등을 이용하여 상황인식을 하고 추론을 통하여 낭비되는 에너지를 줄이거나 특정장소에서 필요한 기능을 자동으로 지원할 수 있는 논리적 추론기법을 제안하였다.

Ⅲ. 지능형 접근제어 서비스를 위한 보안 상황인식

A. 시스템 구성도

전력시스템 접근에 대하여 신속한 대응이 가능하도록 지능화된 접근 제어모델을 위하여 주요 전력시스템에서 적용할 수 있는 보안 상황인식을 위한 온톨로지 구축 방안을 제시하고자 한다. 이를 위해 전력시스템의 보안 취약성을 분석하고 보안상황 온톨로지 및 추론규칙을 설계하여 지능형 접근제어 서비스를 위한 보안 상황인식 구축을 제안한다.



[그림 3-1] 전체 시스템 흐름도

[그림 3-1]은 논문에서 제안하는 전체 시스템 흐름도이다. 스마트그리드 환경에서 보안상황 온톨로지 구축을 위하여 전력시스템의 취약점들을 수집 및 분석하고 보안상황 정보를 추출한다. 전력계통별 전력시스템의 분석된 취약점 데이터와 보안상황들을 기반으로 상황 정보 온톨로지를 모델링하고, 공격상황에 대한 추론규칙을 통하여 추론 엔진을 구축한다. 실험을 통하여 보안침해상황에 대한 추론이 잘 이루어지는지를 확인하였다.

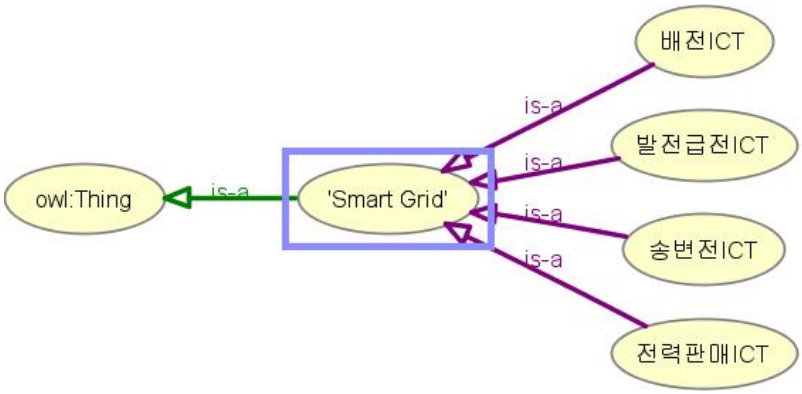
B. 온톨로지 설계 및 구축

1. 전력망 온톨로지

스마트 그리드에서 이용하는 전력시스템들은 전력의 생산에 사용되는 기술부터 안전한 송배전을 위한 기술, 그리고 소비자에게 전력을 제공하는 판매과정에 이용되는 기술들까지 단계별로 여러 종류의 시스템들이 존재한다. 전력망 온톨로지의 구축을 위하여 전력ICT 관련 시스템들을 토대로 구성하였다. 각 단계별 전력시스템들을 클래스로 정의하고 Level 개념을 통해 상위클래스와 하위클래스로 나누었다. 온톨로지 내 모든 Class는 Thing의 하위 개념이고 Level 1은 최상위 클래스를 나타내며 다음 Level로 갈수록 하위클래스를 나타낸다. [표 3-1]와 [그림 3-2]는 Level 1과 Level 2의 정의와 관계를 나타낸다.

[표 3-1] Level 1클래스와 Level 2 클래스 정의

Level	Class	Level	Class
1	Smart Grid	2	발전급전ICT
			송변전ICT
			배전ICT
			전력판매ICT

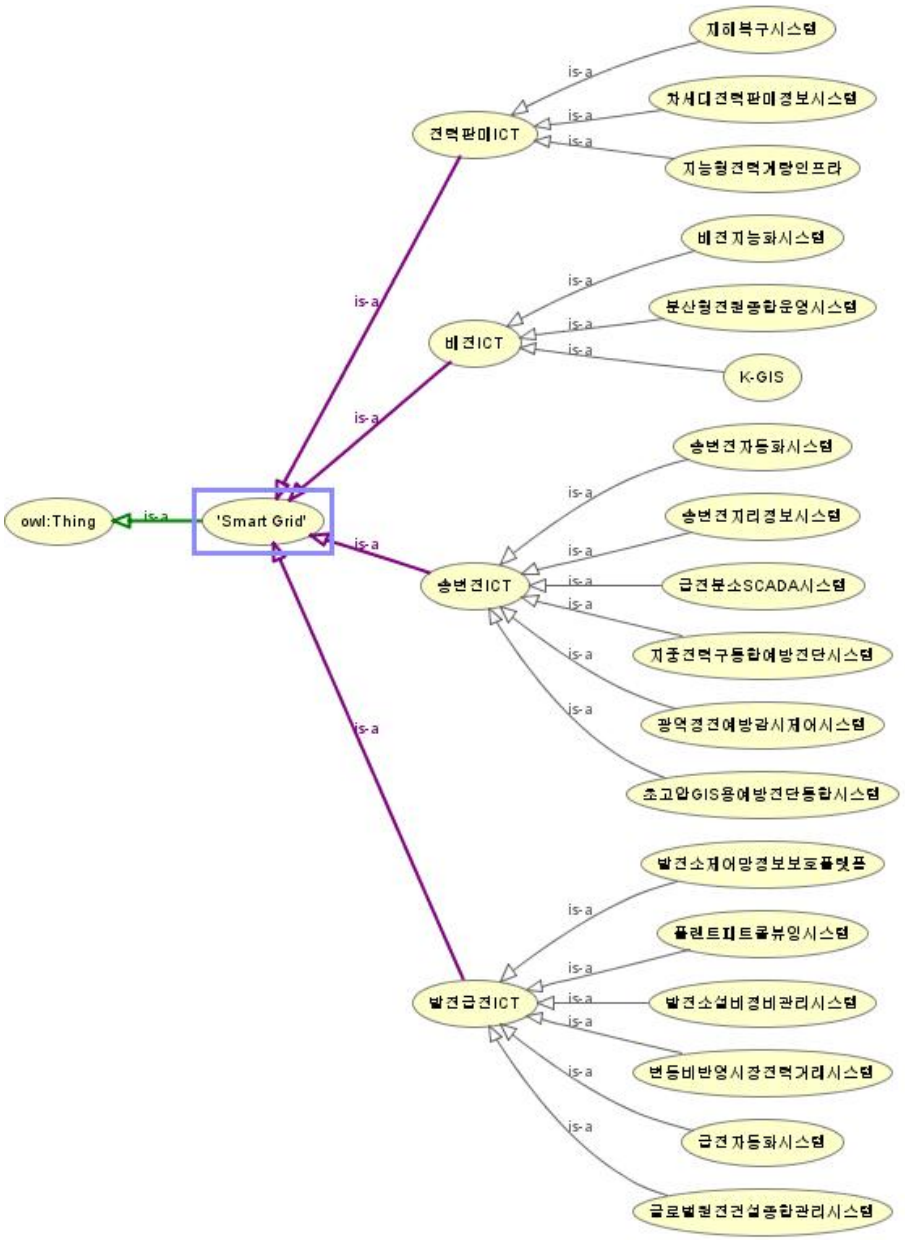


[그림 3-2] Smart Grid Level 1과 Level 2 관계

스마트그리드의 전력망 온톨로지를 구성하기 위해 전력의 생산부터 판매까지 4가지의 하위 클래스를 두었으며 앞에서 클래스를 나누어 정리한 것과 같이 각각 표와 그림으로 Level 2의 클래스를 구성하는 Level 3 단계의 클래스로 나누어 정리하였다.

[표 3-2] Level 2클래스와 Level 3 클래스 정의

Level	Class	Level	Class
2	발전급전ICT	3	플랜트패트롤뷰잉시스템
			발전소제어망정보보호플랫폼
			글로벌원전건설종합관리시스템
			발전설비정비관리시스템
			변동비반영시장전력거래시스템
			급전자동화시스템
2	송변전ICT	3	광역정전예방감시제어시스템
			초고압GIS용예방진단통합시스템
			급전분소SCADA시스템
			지중전력구통합예방진단시스템
			송변전자동화시스템
			송변전지리정보시스템
2	배전ICT	3	배전지능화시스템
			분산형전원종합운영시스템
			K-GIS
2	전력판매ICT	3	재해복구시스템
			차세대전력판매정보시스템
			지능형전력계량인프라



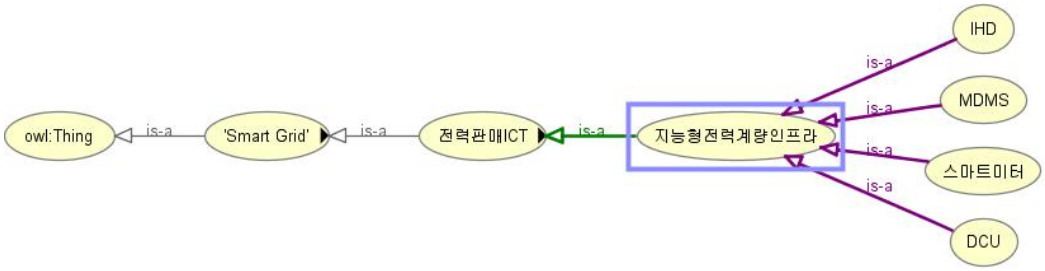
[그림 3-3] 스마트그리드 전력망 온톨로지 관계

스마트그리드의 전력망 온톨로지가 구축되었고 [그림 3-3]과 같이 나타내었다. Level 3 단계 Class를 구축하는 Level 4 단계의 Class도 존재하지만 각 시스템을 구성하는 요소들이 너무 방대하여 Level 3 까지 간추렸다. 간단히 Level 4 단계의 예를 들면 스마드그리드의 핵심 기술이라 불리는 지능형전력계량인프라(AMI) 시스

템으로 표현 가능하다. [표 3-3]와 [그림 3-4]은 Level 3단계와 4단계를 보여주는 AMI시스템의 정의와 관계이다.

[표 3-3] Level 3클래스와 Level 4 클래스 정의

Level	Class	Level	Class
3	지능형전력계량인프라	4	스마트미터
			DCU
			MDMS
			IHD



[그림 3-4] Level 3클래스와 Level 4 클래스 관계

전력망 온톨로지에서의 Level 4 단계의 Class들은 2장에서 설명할 보안 취약점 온톨로지와 연관된 인스턴스로 보안상황 발생 여부를 판단하는 중요한 요소가 된다. 보안 취약점들을 분석하여 정리하고 상황발생시 시스템에 어떠한 영향을 끼칠지를 추론할 수 있다.

2. 전력시스템 보안 취약점 온톨로지

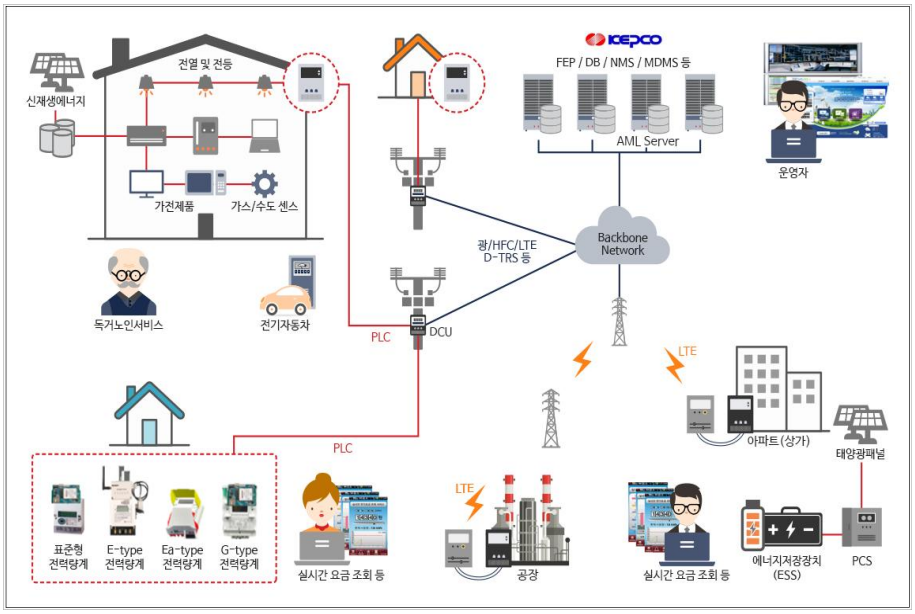
전력시스템들의 보안 취약점들을 수집 및 분석하고 전력망 온톨로지의 연관관계를 통하여 보안상황을 분류할 수 있다. 너무 광범위한 시스템들의 규모와 여러 종류의 취약점들이 모두 표현하기에 어려우므로 스마트그리드의 핵심기술인 AMI 시스템의 보안 취약점을 대상으로 기존에 연구된 보안취약점들을 [표 3-4]와 같이 정리하고 취약점 온톨로지를 표현하였다[21].

[표 3-4] AMI 보안 취약점

취약점	개요
평문 통신	통신 데이터를 암호화하지 않고 평문으로 전송
하드웨어 통신 정보 가로채기	EEPROM으로부터 직접 정보를 획득, I2C버스와 SPI로부터 통신정보를 획득
부적절한 암호기술 사용	키 생성알고리즘 취약점, 키스트림 재사용, 재생공격, 취약한 암호 알고리즘사용, 짧은 키 사용, 부적절한 무결성 검사와 IV 사용 등
직접적인 하드웨어 접근	Tamper-Protection 기능의 취약점을 이용하여 하드웨어에 접근 가능
패스워드와 저장된 키	암호화와 인증 및 무결성 검증을 위해 패스워드와 키가 미터에 저장됨
암호키 분배	검증되지 않은 인증서나 훔친 키로 통신 내용 복호화 가능
안전하지 않은 인터페이스	짧은 거리의 통신을 이용하기 때문에 다른 통신에 비해 덜 위험하다고 생각하며 공격대비 미흡
미터 인증	스마트미터와 NAN장치의 인증에서 잘못된 Nonce값 사용, 재생공격, 서비스거부공격으로 인한 메모리고갈 등 발생가능
NAN 기기 인증	NAN장치는 인증을 받는 절차에 미터 인증 취약점과 동일한 취약점이 존재

펌웨어 구현	Buffer overflow와 Format String과 같이 펌웨어 구현상의 오류를 이용한 공격이 가능함
DNS	스마트그리드 환경에서 사용되는 Name Resolution기법에 Name server Dos 공격, Meter name resolution cache poisoning 등의 취약점 존재
취약한 기본설정정보	일부 기기들은 보안설정을 사용자에게 위임하고 있어 적절한 환경설정이 이루어지지 않는 기기들은 공격에 노출
통신경로	공격자가 중간에 자신을 거치도록 통신경로를 만들어 중간자 공격 가능
서비스거부공격	다른 사용자의 이용을 방해하도록 리소스를 독점하는 Dos 공격 가능
정보누출	특정 정보 등을 평문으로 전송하는 일부 통신에서 정보 유출을 통해 개인 프라이버시를 침해가능
고정된 인증값 사용	변경되지 않은 고정된 인증값을 이용한 공격 가능
난수생성기	무결성 및 기밀성을 보장하기 위한 난수생성기를 구현하는 기술이 어려움
시간서비스	Network Time Protocol, Global Positioning System 취약점을 이용한 공격 가능

AMI 기술 관련 연구에서 취약점을 18종으로 정리하였고 이 취약점들은 각각 다른 개별 취약점이 아니고 인증기술, 암호와 기술, 네트워크 통신관련 기술 등으로 분류할 수 있으며 취약점들의 조합을 통해 수많은 종류의 보안 위협이 만들어질 수 있다. AMI를 구성하는 요소별로 취약점을 구분하기 위해서는 AMI 시스템을 알아야한다. AMI시스템의 주요기능은 소비자의 실시간 전력사용 데이터를 원격 수집하고 변압기의 부하를 감시하며 스마트 미터 기반의 전력정보를 실시간, 양방향으로 소비자와 교환하고 원격으로 제어하며 IoT 통신망을 제공한다. [그림 3-5]는 지능형 전력계량 인프라(AMI)의 구성도이다[22].



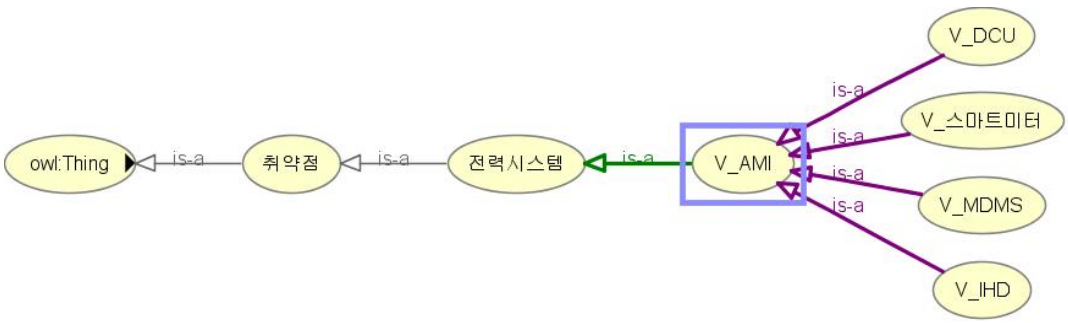
[그림 3-5] AMI 시스템 구성도 (출처:한전KDN)

AMI 시스템의 통신은 크게 2가지가 있는데 스마트미터와 DCU, DCU와 AMI서버간의 통신이다. 가정에서 소비되는 전력량을 스마트미터와 같은 전력량계 측정장치를 통해 DCU와 통신하는데 다양한 유무선 통신방식(PLC, Wi-SUN, ZigBee, LoRa 등)을 통한 DCU의 NAN 구성 및 미터 통신을 지원한다. DCU와 AMI 서버간의 통신은 CDMA와 광통신, Wi-Fi 등 다양한 WAN(Wide Area Network)통신방식을 지원한다. 본 논문에서는 AMI 시스템의 통신과정에서 중요하다고 판단된 시스템의 구성요소를 중점으로 취약점을 정리하였다.

스마트미터는 실시간으로 에너지사용량을 측정하고 소비자와 제공자사이에 양방향 통신을 통해 전력데이터를 제공하도록 설계된 미터기로 스마트미터 제조회사별로 차이가 있을 수 있지만 시간대별 전력사용량을 측정과 원격관리를 통해 기기상태 점검 및 감시를 하고 모니터링과 펌웨어 업데이트 등의 기능을 추가로 지원할 수 있다. 스마트미터의 보안위협은 사용자와 에너지공급업자의 이익창출을 목적으로 한 데이터조작 및 설정변경과 같은 내부공격과 기기의 물리적 접근을 통하여 데이터를 획득 및 시스템 권한 획득과 같은 외부공격을 예상할 수 있다.

DCU(Data Control Unit)는 데이터 집중 장치로 전력선 통신방식(PLC), Zigbee, LTE 등을 이용해 수용가 측 스마트 전력량계로부터 검침정보를 수집, 저장하고 전력 공급자에게 전송하며 전력 소비자와의 양방향 수요반응을 통해 에너지 발전, 사용의 효율을 높이는 스마트그리드 원격검침 인프라의 핵심장비이다. 계기자동등록, 변압기 부하 감시, 원격 소프트웨어 업그레이드, 간선망 공유를 통한 DCU간 데이터 연계 등의 기능을 한다. PLC통신의 유선망과 Zigbee, WiSUN, LTE 등의 무선통신을 이용하여 통신한다. 물리적 공격으로부터의 취약점이 존재하는데 메모리 덤프 등을 통해 DCU에 저장된 중요정보가 노출될 수 있고 관리자권한을 획득할 수 있다. 디폴트 패스워드 설정과 같이 부적절한 계정 관리도 문제가 될 수 있다.

MDMS(Meter Data Management System)는 전력정보관리시스템으로 DCU를 통해 실시간으로 수집된 전력데이터를 처리, 가공, 분석해 가치 있는 정보로 변환시켜 요금서비스 및 다양한 부가서비스 창출에 활용된 소프트웨어 인프라로 AMI의 로그정보들을 저장한다. MDMS 시스템은 전용망으로 연결 되어 있기 때문에 직접적인 침투가 어렵지만 침투하게 되면 악의적인 DCU와 스마트미터 제어가 가능해진다. 시스템에서 사용되는 운영체제 및 어플리케이션에 대한 취약점 분석 수행을 통한 간접 침투을 예방해야 하는데 사용자관리 앱 서비스의 취약점과 계량정보를 저장하는 DB 서버의 취약점, 스마트 기기와 연동을 위한 앱 서비스의 취약점을 통한 공격을 조심해야 한다.

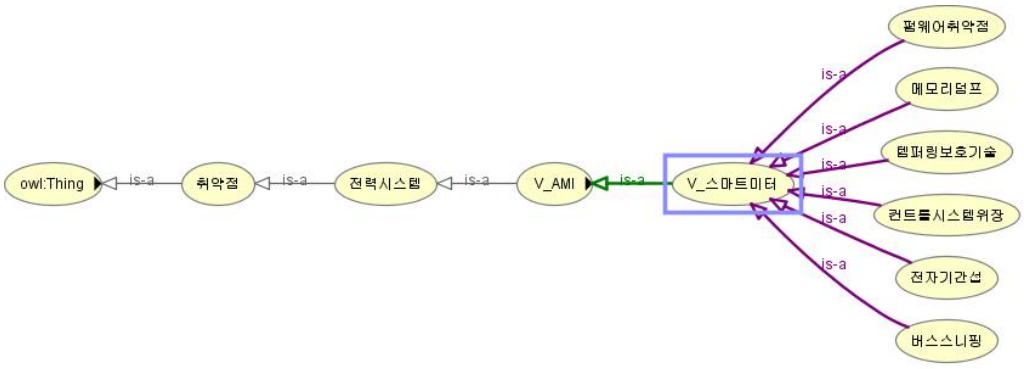


[그림 3-6] 취약점 온톨로지 관계

[그림 3-6]의 취약점 온톨로지는 AMI를 구성하는 4가지 요소에 대하여 표현하였는데 앞에서 설명한 AMI 취약점들은 각각 네트워크상에서 이용되는 기술을 이용한 사이버공격부터 전자기기 및 하드웨어와 같은 물리적 공격, 담당자 및 관리자의 미숙한 관리와 같은 위협요소들이 포함된다. [표 3-5]는 AMI의 4가지 구성요소에 연관되어 스마트그리드를 위협하는 요소로 정리하였다.

[표 3-5] AMI 구성요소별 관련 취약점

AMI 구성요소	취약점
스마트미터	메모리덤프, 버스 스니핑, 펌웨어 취약점, 템퍼링보호기술, 컨트롤 시스템 위장, 전자기간섭 등
DCU	저장된 정보 노출, 전수공격 관리자권한 획득, 물리적 공격 취약점, 관리 S/W 공격 등
MDMS	웹서비스취약점, DB서버취약점, 앱 서비스 취약점, 부적절한 계정관리
통신프로토콜	패킷 스니핑 및 조작, 세션하이재킹, DOS, 재전송, 접근 프로토콜을 이용한 디바이스 공격



[그림 3-7] 스마트미터 취약점 온톨로지 관계

이들을 살펴보면 스마드그리드 보안 위협은 크게 4가지로 펌웨어조작, 램공격, 네트워크 공격, 서비스 거부 공격 등으로 정리된다. 보안기능을 갖는 기기들은 암호화를 위해 펌웨어 형태로 암호 키를 내장하게 된다. 펌웨어를 해독한다면 장치에 설정되어 있는 암호 키를 알 수 있어 모든 정보가 유출될 수 있는 위험이 존재한다. 전자기기의 메모리 칩에 바늘을 사용하여 메모리 칩의 전기신호를 가로채는 램 공격은 스마트미터기의 전기신호를 가로채고 신호를 분석하여 사용자의 에너지 사용정보를 알수 있고 프로그램을 조작하여 정보를 왜곡시킬 수도 있다. 스마트미어의 프로그램을 해킹할 수 있다면 웜과 같은 악성코드 설치가 가능해지고 전력 네트워크망에 악성코드가 전파될 수 있다. 건물 내부망이나 서버와 송수신하는 외부망처럼 어떤 전력망이 해킹되느냐에 따라 피해는 걷잡을 수 없이 커질 수 있다. 네트워크망에 연결된 스마트미터 및 전력관력 전자기기 등의 모든 오작동을 유발하며 트래픽을 증가시켜 정상적인 서비스가 불가능한 서비스 거부공격까지 가능하게 된다.

C. 추론규칙 설계

접근 제어 추론 엔진의 추론규칙 설계는 매우 중요하다. 스마트그리드의 전력시스템은 하나의 시스템에 국한되는 것이 아니라 다양하고 수많은 전력시스템들이 합쳐진 형태의 거대한 네트워크망이라고 할 수 있다. 그렇기 때문에 스마트그리드의 전력시스템에 대한 공격 또한 수많은 경로와 다양하고 복합적인 공격방법들에 대한 위협이 존재한다. 이를 위해 취약점을 통한 공격방법과 공격목표인 시스템까지의 경로를 고려하여 추론규칙을 설계해야한다. 본 연구에서는 AMI 취약점을 이용한 공격단계와 목표 시스템까지의 접근경로 등에 해당되는 상황을 고려하여 추론규칙을 설계하였다.

AMI시스템에서 취약점을 이용한 공격방법은 스마트미터와 같은 전력관련 전자기기의 통신상에서의 공격과 물리적 접근을 통한 공격이 있다. 물리적 접근을 통한 취약점은 기기 설치시 쉽게 접근하기 어려운 위치 선정 및 보관과 같은 관리적 차원에서 충분히 위험을 낮출 수 있기 때문에 추론에서 제외하고 네트워크 통신 및 프로토콜에 관한 취약점에 대하여 [표 3-6]과 같이 추론규칙을 정의하였다.

[표 3-6] 취약점 공격 추론규칙

공격 상황	추론 규칙
패킷 스니핑	(?T behaviour Packet_Sniffing) ∧ (Packet_Sniffing resultIn Key_Acquisition) ∧ (Key_Acquisition resultIn Data_Gathering) => (?T MITM ATTACK)

취약점 공격단계에서 중간자공격의 행위로 패킷 스니핑을 이용하였다. 스마트미터와 같은 전력기반 전자기기의 무선 통신 구간에서 패킷을 가로채는데 이 패킷을 가지고 전수조사와 같은 암호화 키 해독기법을 이용하면 전자기기상에 인증 및 암호화키를 획득할 수 있다. 키 획득 이후 데이터를 복호화하여 전력사용 데이터를 수집 및 분석할 수 있게 된다.

[표 3-7] 공격 단계 추론 규칙

공격 상황	추론 규칙
시스템 접근	(?T behaviour Key_Acquisition) ∧ (Key_Acquisition resultIn Data_Gathering) ∧ (Data_Gathering resultIn System_Access) => (?T BACK DOOR)

취약점 공격의 다음단계에서 데이터를 수집하고 분석한다면 전력사용자의 생활패턴을 알 수 있고 프라이버시 침해가 가능해진다. 그리고 획득한 키로 인해 동일 네트워크상에 있는 다른 기기에 영향을 줄 수 있으며 연결된 네트워크를 통해 다른 전력시스템으로 접근이 가능해진다.

[표 3-8] 공격 결과 추론 규칙

공격 상황	추론 규칙
시스템 공격	(?T behaviour Data_Gathering) ∧ (Data_Gathering resultIn System_Access) ∧ (System_Access resultIn System_Control) => (?T SYSTEM ATTACK)

키 획득 이후 정보를 수집하여 백도어 및 원격접속을 통하여 시스템에 접근한다. 전력제어시스템을 조작하여 시스템을 공격할 수 있는데 이 과정에서 공격자는 서버에 접근하고 기밀정보 등을 유출할 수 있으며 시스템의 동작을 방해하거나 Shutdown과 같은 공격을 통해 시스템을 파괴 할 수도 있다.

Ⅳ. 실험 및 평가

A. 보안 침해상황 시나리오

본 장에서 제안하는 스마트그리드 보안 상황인식을 위한 지능형 접근제어 서비스의 성능을 측정하기 위해 실제상황에서 일어날 수 있는 공격패턴의 상황을 시나리오로 구성하였다.

[표 4-1] 보안상황 시나리오 구성

시나리오
AMI 시스템 근무자 'B'씨는 며칠 전 직장생활을 위해 타지에서 혼자 자취하는 'C'씨에게 전기세가 갑자기 3배가량 나왔다고 확인을 요청하는 민원을 받았다. 평소와 달리 증가된 전력사용량을 확인 한 'B'씨는 별다른 원인을 찾지 못한 채 휴가를 갔고 며칠 후 AMI 시스템 근무자 'A'씨는 전력제어시스템이 다운되었다는 갑작스러운 호출을 받았다. 전력제어시스템은 안전한 운영을 위해 인터넷망과 분리된 폐쇄망으로 운영하고 있기 때문에 회사에 출근하여 시스템을 확인하였다. 서버와 시스템이 다운되어 있었고 시스템을 재부팅하고 이상이 있는지 확인했는데 특별한 이상이 없었다. 갑작스러운 시스템 다운의 이유를 찾기 위해 로그를 확인해보는데 휴가 중인 'B'씨가 Shutdown 명령을 내린 기록이 있다. 하지만 B씨는 휴가 중으로 회사에 있지 않았는데 과연 어떻게 된 것일까?

보안 침해상황 시나리오 정보를 기반으로 추론엔진을 이용하기 위해 온톨로지에서 클래스를 추출하였다. [표 4-2]는 시나리오기반 상황추론을 위한 시스템관리자의 대응에 대하여 정리하였다. AMI 시스템에서 갑작스러운 전력사용량 증가와 같이 원인을 알 수 없는 상황에서 취약점을 이용한 공격을 의심하고 전력제어시스템 다운을 통해 Shutdown과 같은 시스템공격을 의심하고 공격자의 시스템 접근 및 제어에 대하여 확인해 볼 수 있다.

[표 4-2] 시나리오기반 상황추론

상황 정보	대응
일인가정에서 전기세가 갑자기 3배가량 나왔다고 확인을 요청하는 민원을 받았다.	취약점 공격 의심
전력제어 시스템의 서버가 다운되어 있었고 시스템을 재부팅하고 이상이 있는지 확인했는데 특별한 이상이 없었다.	시스템 공격 의심
휴가 중인 'B'씨가 Shutdown 명령을 내린 기록을 확인하였다.	시스템 접근 및 제어 확인

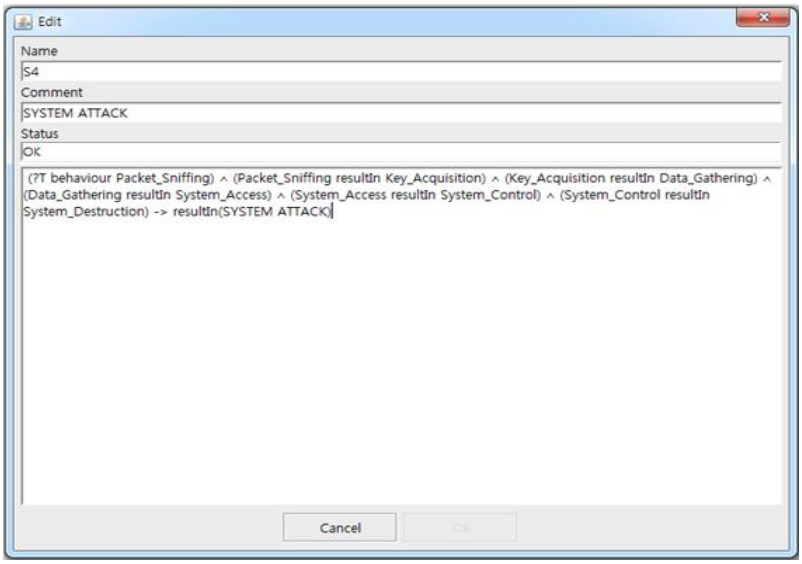
가정 내 전력정보를 위한 네트워크에서 스마트미터 및 스마트센서와 통신은 무선 통신을 사용하는데 펌웨어취약점을 이용하거나 램 공격처럼 스니핑 도구를 이용한 패킷 스니핑을 시도하고 패킷을 획득할 수 있다. 획득한 패킷을 이용하여 암호화 키 해독기법을 이용하여 인증 및 데이터 암호화를 위한 키를 획득할 수 있다. 이후 데이터를 복호화하여 사용자의 전력 데이터를 수집할 수 있고 사용자의 생활패턴 분석을 분석하는 프라이버시 침해 발생이 가능해진다. 또한 동일 네트워크 상에 있는 다른 기기에 영향을 줄 수 있으며 전력공급과 같은 시스템의 조작 및 제어가 가능해진다. 보안 침해상황 시나리오에서 SWRL언어 기반으로 단계별 추론식을 정의하고 시스템 공격에 대하여 추론식을 도출한 결과를 [표 4-3] 정리하였다.

[표 4-3] 보안상황 시나리오 기반 추론식

취약점 공격	(?T behaviour Packet_Sniffing) ∧ (Packet_Sniffing resultIn Key_Acquisition) ∧ (Key_Acquisition resultIn Data_Gathering) => (?T MITM ATTACK)
시스템 접근	(?T behaviour Key_Acquisition) ∧ (Key_Acquisition resultIn Data_Gathering) ∧ (Data_Gathering resultIn System_Access) => (?T BACK DOOR)

시스템 조작	(?T behaviour Data_Gathering) ∧ (Data_Gathering resultIn System_Access) ∧ (System_Access resultIn System_Control) => (?T REMOTE ACCESS)
시스템 공격	(?T behaviour System_Access) ∧ (System_Access resultIn System_Control) ∧ (System_Control resultIn System_Destruction) => (?T SYSTEM ATTACK)

실험을 위해 온톨로지 구축을 위해 Protégé 에 내장되어있는 SWRL 추론엔진을 이용하여 추론식을 작성하였다. 공격은 여러 단계에 걸쳐 복합적으로 동작하며 탐지를 위한 추론식은 [그림 4-1]과 같이 구성하였다.



[그림 4-1] SWRL을 이용한 추론식

구축된 온톨로지 시스템에 실제상황에서 일어날 수 있는 공격패턴의 보안침해상황 시나리오를 통해 SWRL 규칙을 이용하여 추론식을 작성하였다. 이 경우 시나리오에 맞게 준비된 추론식을 통해 시스템에 추론이 가능하다는 결과는 확인할 수

있었다. [표 4-4]는 실험에 사용된 시나리오에 대한 보안상황들과 미리 준비한 20개의 추론 규칙에서 인식된 추론규칙의 수와 그에 대한 상황인식률을 정리하였다.

[표 4-4] 추론상황 성능비교

공격 시나리오	보안 상황정보	인식된 추론규칙	상황 인식률
스마트 그리드	스니핑, 키획득, 데이터복호화, 백도어, 원격 접속, 데이터갈취, 시스템접속, 시스템 제어, 시스템 파괴 등	16	80%
	(?T behaviour Packet_Sniffing) ∧ (Packet_Sniffing resultIn Key_Acquisition) ...		
스마트미터	마이크로컨트롤러와 펌웨어조작, 램 공격, 설정변경, 물리적인 해킹, 보안코드 획득, 네트워크 접근, 시스템 파괴 등	12	60%
	(?T behaviour Firmware_Attack) ∧ (Firmware_Attack resultIn Setting_Change) ...		
DCU	템퍼링 보호기술, 시리얼 포트, 시스템접속, 디폴트 패스워드, 전수 공격, 관리자 권한 획득, 시스템 제어, DDoS 공격 등	15	75%
	(?T behaviour Tampering_Attack) ∧ (Tampering_Attack resultIn Key_Acquisition) ...		
MDMS	관리자 USB, 스턱스넷, 관리자 PC에 설치, 백도어, ARP 스푸핑, 중간자공격, 패킷스니핑, 명령어 조작, 시스템 제어 등	8	40%
	(?T behaviour resultIn Malware_Stuxnet) ∧ (resultIn Malware_Stuxnet resultIn System_Access) ...		

여러 상황의 시나리오를 준비하고 추론식을 늘려 여러 가지 상황에서 어떠한 추론규칙으로 추론이 동작하는지 수치를 확인 할 수 있지만 시스템에 대한 공격은 매우 다양한 공격방법과 공격방법에 맞는 공격단계가 변칙적으로 바뀌기 때문에

실제 여러 상황에서 어떠한 확률로 추론이 가능한지에 대한 객관적인 성능 비교를 하는데 어려움이 있다고 판단된다. 본 논문에서 제안하는 보안 상황인식을 위한 온톨로지 모델과 관련연구에서 설명한 온톨로지기반 상황인식모델들을 비교하여 평가하였다.

[표 4-5] 온톨로지 상황모델 비교

구분	CoBrA	CONON	제안모델
카테고리		○	○
상속성	○	○	○
결합력	○		○
확장성		○	○
정형성	○	○	○
재사용성			○
DL추론	○	○	○
규칙추론			○

온톨로지기반 모델은 상호 관계성 및 부분적인 상황정보를 쉽게 표현하고 RDF, OWL 등의 온톨로지 표준 언어로 선언적인 표현이 특징이며 상위계층 하위계층 온톨로지를 이용한다. 규칙이 많아지면 복잡해지는 단점이 있으며 상황온톨로지만 정의하고 시스템의 서비스와 운영과 같은 동적 서비스 적용을 고려하지 않아 상황인식시스템의 상황 지식베이스 구축에 부족하다. 기존의 상황인식시스템구조는 분산 상황인식시스템에 적합하고 상황모델은 온톨로지 모델을 적용하여 해당 추론기를 사용한다. 하지만 DL 추론과 같이 논리적 추론만을 제공한다. 반면 본 논문에서 제공하는 모델은 SWRL언어를 사용하여 규칙을 만들고 규칙기반 추론기능을 추가하였다.

V. 결론 및 제언

본 논문은 스마트그리드 상황에서 시스템 취약점을 수집 및 분석하고 온톨로지를 구축하여 보안 침해에 대비할 수 있는 지능형 접근제어 서비스를 위한 보안 상황인식을 목적으로 하였다. 논문에서 제안하는 보안 상황인식 온톨로지 설계를 위해 전력ICT 솔루션 전력계통에 따라 전력시스템들을 정리하였고 전력의 발전부터 급전, 송변전, 배전, 판매까지의 과정에서 필요한 주요 솔루션 및 시스템들과 시스템별 취약점들을 수집하고 분석하여 취약점을 기반으로 상황인지 모델링에 초점을 두었다. 이를 위하여 전력시스템과 취약점과의 매칭뿐만이 아니라 전력시스템의 요소별 관계를 정의하고 의미적 접근법을 이용한 온톨로지를 구축하였다. 또한 취약점별 공격의 형태와 공격 경로까지 생각하여 공격 전후 환경에 대하여 지식 정보의 기초를 정의하였다.

실험은 실제상황에서 일어날 수 있는 공격패턴의 상황시나리오를 통해 AMI 시스템의 취약점을 이용한 공격과 단계별 공격경로를 확인하는 추론규칙을 작성하고 추론식을 통하여 공격을 확인할 수 있었다. 시스템에 대한 공격은 다양한 공격방법과 그에 따른 공격단계가 변칙적으로 바뀌기 때문에 실제 여러 상황에서 어떠한 확률로 추론이 가능한지에 대한 수치화되고 객관적인 성능 비교를 하는데 어려움이 있다. 논문에서 제안하는 보안 상황인식을 위한 온톨로지 모델과 기존의 온톨로지기반 상황인식모델들을 비교하여 평가하였다.

본 논문에서 제안하는 시스템 및 기술은 기존의 다른 연구들에 비해 SWRL 언어를 이용한 규칙추론을 추가하여 의미적 추론뿐만 아니라 규칙기반의 추론으로 보안 침해상황을 이해하는 추론이 가능해졌다. 실험을 하면서 아쉬웠던 점은 여러 상황의 시나리오와 그에 맞는 추론식을 준비하여 추론이 동작하는지는 확인 할 수 있지만 규칙이 많아질수록 복잡해지는 단점이 있었다. 전력시스템을 이해하고 그에 따른 보안침해상황을 예상하고 준비하려면 추론 규칙이 반드시 필요하기 때문에 시스템의 확장성을 위하여 시스템별 취약점과 같이 카테고리를 나누어 추론규칙을 정의하는 과정이 추가되어야 할 것 같다.

향후 연구로는 스마트그리드를 구성하는 전반적인 시스템에 관련된 취약점들을 추가 조사하여 추론 규칙을 수정하고 보안하여 추론식의 다양성을 갖추고 기존에

설계한 온톨로지와의 매칭을 통해 다양하고 복합적인 공격 및 보안 위협에 대해 탐지만을 하는 것이 아니고 더 나아가 복잡하고 다양한 보안 상황을 인식하고 이에 알맞은 대응까지 하는 것을 목표로 한다.

참고문헌

[1] 장기윤, “2017년 국내외 에너지시장 전망” POSRI 이슈리포트, 2017.

[2] 도윤미, 김선진, 허태욱, 박노성, 김현학, 홍승기, 서정해, 전종암. “스마트 그리드 기술 동향:전력망과 정보통신의 융합기술” 전자통신동향분석, 제 5호, 2009.

[3] 박찬국, 용태석, “스마트그리드 기술 및 시장 동향” 과학기술 및 연구개발사업 동향브리프, 2011.

[4] 유재국, “스마트그리드 사업의 현황과 개선 과제” NARS 현안보고서, 제 294호, 2016.

[5] 지식경제부, “스마트그리드 국가로드맵” 2010.

[6] 한국방송통신전파진흥원, “스마트그리드에서의 취약성 보안 기술” 방송통신기술 이슈&전망, 제 28호, 2013.

[7] 이성진, “전력IT제어시스템에 대한 사이버공격 대응방안을 위한 연구” 고려대학교 석사학위논문, 2016.

[8] 지식경제부, “에너지기후변화 주요 경제국포럼(MEF) 스마트그리드 로드맵 수립” 전력정책연구보고서, 2009.

[9] 유성민, 김남균, 김윤기, “스마트그리드 보안기술 동향분석 및 대응방안” ICT Security, 2014.

[10] 스마트그리드협회, http://www.ksga.org/sub2/sub01.asp

[11] 스마트그리드사업단, https://www.smartgrid.or.kr/page.php?id=sub5_1

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

[13] 이명호, 홍석원, 이철환, 임일형, 최규영, “클라우드기반 스마트 그리드를 위한 보안기술 연구” 한국인터넷진흥원, 2010.

[14] 고호준, 김휘강, “발전소 주제어시스템 모의해킹을 통한 취약점 분석 및 침해사고 대응기법 연구” 정보보호학회논문지, 제 2호, 2014.

[15] 한국전산원, “웹 온톨로지 개발지침 연구” 2004.

[16] 이승우, 정한민, 김평, 서동민, “추론기술연구동향” 정보통신산업진흥원 2010.

[17] 김수경, 안기홍 ″기술논리와 SWRL기반의 웹 온톨로지 모델링″ 정보관리학회

지, 제 25권, 제 1호, 2008.

[18] 홍충성 "상황인식 프레임워크를 위한 온톨로지 기반 상황정보 모델링 방법론" 홍익대학교 박사학위논문, 2007.

[19] H. Chen, T. Finin, A. Joshi, “Semantic Web in the context broker architect ure” Pervasive Computing and Communications, 2004.

[20] X.H. Wang, D.Q. Zhang, T. Gu, H.K. Pung, “Ontology based context mode ling and reasoning using OWL” Pervasive Computing and Communications Workshops, 2004.

[21] 김신규, 전유석, 서정택. “AMI 보안 취약점 점검 항목에 관한 연구” 정보보호 학회지, 2012.

[22] 한전KDN “https://www.kdn.com/menu.kdn?mid=a10204070000”