JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 28 No. 5, pp. 57-66, May 2023
https://doi.org/10.9708/jksci.2023.28.05.057

Feasibility Analysis on the Attack Graph Applicability in Selected Domains

Junho Jang*, Saehee Jun*, Huiju Lee*, Jaegwan Yu**, SungJin Park**, Su-Youn Hong**, Huy Kang Kim*

*Student, School of Cybersecurity, Korea University, Seoul, Korea
*Student, School of Cybersecurity, Korea University, Seoul, Korea
*Student, School of Cybersecurity, Korea University, Seoul, Korea
**Research engineer, LIGNex1, Seongnam, Korea
**Research engineer, LIGNex1, Seongnam, Korea
**Chief research engineer, LIGNex1, Seongnam, Korea
*Professor, School of Cybersecurity, Korea University, Seoul, Korea

[Abstract]

In this paper, a research trend of attack graph studies for Cyber-Physical System (CPS) environments is surveyed, and we analyse the limitations of previous works and prospect the future directions. 35 among around 150 attack graph studies conducted within 5 years target CPS, and we inspect key features of CPS environment in the security aspect. Also, we categorize and analyze target studies in the aspect of modelling physical systems and considering air gaps, which are derived as key features of the security aspects of CPS. Half of 20 research that we surveyed do not reflect those two features, and other studies only consider one of the two features. In this circumstance, we examine challenges that attack graph studies on CPS environment face. Finally, we expect state-led studies or studies targeting open-spec commercial CPS will dominate.

▸ **Key words**: Attack graph, CPS, Cloud, System modelling, Threat modelling

[요 약]

본 논문에서는 Enterprise 네트워크 이외 환경에서의 공격 그래프 연구 중 최근 5년간 가장 많이 연구된 사이버-물리 시스템(CPS) 환경에 대한 공격 그래프 연구 동향을 살펴보고, 기존 연구의 한계와 앞으로 나아갈 방향을 분석한다. 최근 5년간 발표된 공격 그래프 논문 150여 편 중 35편이 CPS 환경을 대상으로 하고 있으며, 본 논문에서는 CPS 환경의 보안 측면 특징을 살펴보고, 대상 연구들을 이러한 특징들에 따라 물리 시스템 모델링 여부와 네트워크 단절 구간에 대한 고려 여부의 두 가지 관점으로 분류 및 분석한다. 본 논문에서 소개한 20편의 논문 중 절반이 CPS 환경의 특징을 제대로 반영하지 못하며, 나머지 절반의 연구가 물리 시스템 모델링과 네트워크 단절 구간 중 하나씩을 다루고 있다. 본 논문에서는 이러한 상황을 바탕으로 CPS 환경에서의 공격 그래프 연구가 직면한 어려움을 진단하고 이에 따라 앞으로의 CPS 환경 공격 그래프 연구는 국가 주도 연구, 공개된 상용 시스템을 대상으로 한 연구가 주를 이룰 것으로 분석한다.

▸ **주제어**: 공격 그래프, CPS, Cloud, 시스템 모델링, 위협 모델링

• First Author: Junho Jang, Corresponding Author: Huy Kang Kim
*Junho Jang (hkonly@korea.ac.kr), School of Cybersecurity, Korea University
*Saehee Jun (junsaehee@korea.ac.kr), School of Cybersecurity, Korea University
*Huiju Lee (kkj0118@korea.ac.kr), School of Cybersecurity, Korea University
**Jaegwan Yu (jaegwan.yu@lignex1.com), LIGNex1
**SungJin Park (sungjin.park2@lignex1.com), LIGNex1
**Su-Youn Hong (suyoun.hong@lignex1.com), LIGNex1
*Huy Kang Kim (cenda@korea.ac.kr), School of Cybersecurity, Korea University
• Received: 2023. 04. 21, Revised: 2023. 05. 10, Accepted: 2023. 05. 11.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

공격 그래프(Attack Graph)는 특정한 네트워크 시스템을 대상으로, 공격자가 정해진 목적을 달성하기 위해 취할 수 있는 가능한 사이버 공격 시퀀스를 모델링하는 기법이다. 네트워크 시스템을 운영하는 기업과 조직은 모델링 된 공격들에 대한 분석을 통하여 한정된 자원으로 가장 효과적인 보안 조치를 수행할 수 있다.

Philips 등은 공격 그래프의 개념을 최초로 제안하였으며[1], Jha 등[2]과 Sheyner 등[3]은 각각의 연구에서 Symbolic Model Checker를 사용한 공격 그래프 생성 기법을 제안하였다. 2005년 발표 된 MulVAL 프레임워크[4]는 논리 언어인 Datalog 문법을 기반으로 네트워크 호스트와 취약점, exploit 사이의 관계를 정의하고, 이를 통해 공격 그래프를 생성한다. 이러한 연구들은 사실적인 공격 그래프를 생성하는 데 초점을 맞추고 있다.

한편, 공격 그래프를 생성하는데 소요되는 컴퓨팅 자원과 연산시간을 줄임으로써 보다 대규모의 네트워크에 대한 공격 그래프(Scalable attack graph)를 생성하거나, 토폴로지의 변화에 빠르게 대응할 수 있는 알고리즘을 개발하는 연구도 수행되었다. 이러한 연구로는 공격 그래프를 네트워크 호스트 간, 각 호스트 내부의 2계층으로 분리하여 생성하는 HARMS 모델을 제안한 Hong 등의 연구[5], 병렬 연산을 통해 공격 그래프 생성 시간을 단축시키고자 한 Kaynar와 Sivrikaya의 연구[6]가 있다.

그러나 위와 같은 연구들에서는 생성된 공격 그래프를 통해 네트워크 시스템에 어떠한 보안 대책을 세워야 하는지에 대한 가이드를 제공하지 않기 때문에, 여전히 대상 시스템에 대한 보안 분석을 위해 전문가의 지식이 많이 필요하다. 때문에 공격 그래프 연구는 그래프를 통해 도출된 공격 경로들의 심각도를 측정하고, 이에 따라 적절한 방어 대책을 세우는 방법을 연구하는 방향으로 발전하였다.

공격 그래프를 생성하는 방법으로 많이 사용되는 것 중 하나는 시스템의 상태와 공격자의 침투 경로를 조건부 확률 모델에 기반하여 나타내는 베이지안 공격 그래프(Bayesian Attack Graph)이다[7]. 베이지안 공격 그래프 모델에서는 공격 경로상의 각 공격에 대한 확률 연산을 통해 각 공격 경로를 평가한다[8]. 이때 각각의 개별 단위 공격(atomic attack)의 성공 확률을 더욱 객관적으로 정의하기 위해 CVSS를 사용하기도 하는데[9], Gallon 등, Keramati 등의 연구처럼 베이지안 공격 그래프가 아닌 형태의 공격 그래프에서도 그래프상의 노드와 엣지의 중요도(가중치)를 판단하기 위해 CVSS를 적용할 수 있다[10-11].

Lu 등은 공격 그래프에 그래프 신경망 (Graph Neural Network, GNN)을 적용하여 그래프상의 각 노드에 대한 순위 (Ranking)을 측정하는 방법을 제안했다[12]. 이 연구는 실제 공격 그래프가 아닌 Pseudo 공격 그래프를 사용했다는 점에서 한계가 있지만, 공격 그래프를 평가하는 데 CVSS와 같은 추가 정보를 사용하지 않았다는 점에서 주목할 만하다.

앞서 언급한 연구를 포함하여 공격 그래프 분야의 연구가 많이 이루어졌지만, 많은 연구들이 Enterprise 환경을 대상으로 공격자의 침투 경로를 분석하는 데 집중되어 있었으며, 지금까지 사물 인터넷 (Internet of Things, IoT)이나 산업제어 시스템(Industrial Control System, ICS)의 사이버-물리 시스템(Cyber-Physical System, CPS)과 같이 망분리 등 특수한 네트워크 환경을 고려한 연구는 많이 이루어지지 않았다.

이에, 본 논문에서는 Enterprise 네트워크 외의 공격 그래프 연구 동향을 살펴보고, 그중 CPS 관련 연구의 주요 연구 방향과 한계, 앞으로의 발전 방향을 살펴보았다.

본 논문의 구성은 다음과 같다. 2장에서 조사 대상이 되는 논문을 선정한 방법과 이유를 설명한다. 3장에서는 CPS에 대한 설명과 보안 분야에서의 특징을 다루며, 4장에서 CPS를 다루는 공격 그래프 연구를 본 논문에서 정한 기준에 따라 분류하여 소개한다. 5장과 6장에서는 CPS 환경에서의 기존 공격 그래프 연구의 한계와 CPS에서의 공격 그래프 연구가 직면한 과제를 분석하고 7장에서 이 분야 연구가 나아갈 방향을 예측한다. 마지막으로 8장에서 결론으로 끝을 맺는다.

II. Literature selection

먼저 최근 5년간 (2019-2023) 공격 그래프 분야 연구 중 enterprise 이외의 네트워크 (non-enterprise network)를 대상으로 한 연구의 학회 발표 또는 저널 게재 현황을 조사하였다. 조사 대상 논문 검색은 Web of Science[13], ACM Digital Library[14], IEEE Xplore[15]를 이용하였는데, 조사 대상이 공격 그래프 분야에 관한 연구이므로 'Attack graph' 키워드와 공격 그래프와 유사한 'Attack tree' 키워드를 검색하였다. 또 공격 그래프를 다루는 경우는 많지 않지만, 공격 그래프 연구 분야와 교집합이 있는, 위협 분석 및 모델링 분야에서의 논문을 탐색하기 위해 'Threat analysis', 'Threat modelling' 키워드도 사용하였다.

위의 방법으로 수집한 조사 대상 중 실제로 공격 그래프 또는 공격 트리를 다루고 있는 논문은 총 154편이며, 이 중 Enterprise 네트워크를 대상으로 한 논문은 83편이다. 나머지 총 71편의 연구 중 CPS를 대상으로 한 논문이 35편으로 가장 큰 비중을 차지하고 있으며 Cloud, IoT 관련 연구가 각각 19편, 10편으로 그 뒤를 잇는다. 나머지는 블록체인, 전자 투표 시스템 등 특수한 도메인을 다루고 있는 소수의 연구이다. Fig. 1.은 식별된 논문 중 각각의 도메인이 차지하는 비중을 나타낸다.

본 논문에서는 non-enterprise network에 대한 공격 그래프 연구 중, 근 5년간 가장 많은 연구가 이루어진 분야인 CPS를 대상으로 한 논문들을 다룬다. 지면의 한계로 조사한 35편의 논문을 모두 수록하지는 못하였으나, 인용 수와 게재·발표된 저널 및 컨퍼런스, 독창성 등을 종합적으로 고려하여 20개의 논문을 선정하여 본문에서 다루었다.

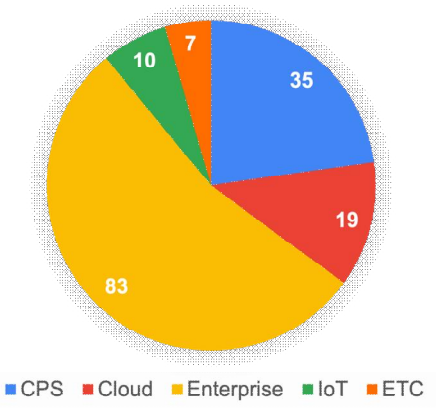

Fig. 1. Target systems of papers about Attack Graph

III. Cyber-Physical System (CPS)

CPS는 컴퓨팅, 네트워킹, 그리고 물리적 프로세스가 하나로 통합된 시스템이다[16]. CPS에서는 컴퓨팅 장치가 센서나 모터와 같은 물리적 장치들로부터 정보를 수집하거나 이들을 제어한다는 점에서 일반적인 정보통신 시스템(서비스)과 차이가 있다. CPS에는 정유소, 발전소와 같은 기반 시설 시스템이나 로봇 제어시스템 등이 있다.

CPS에 대한 대표적인 사이버 공격으로는 이란 핵시설의 원심분리기 천여 기를 파괴했던 Stuxnet이 있다[17]. Stuxnet 의 사례에서 눈여겨 볼 점은 크게 두 가지인데, 첫째로 사이버 공격을 통해 핵시설에 피해를 입힌 방식이다. 기존의 Enterprise 네트워크에 대한 사이버 공격은 주로 중요한 데이터를 탈취 (기밀성 침해) 또는 변조 (무결성 침해) 하거나 또는 서비스 거부 (Denial of Service, DoS)를 통해 서비스가 제대로 동작하지 못하도록 (가용성 침해) 하는데 목적을 두었다. 반면 Stuxnet은 목표 지점까지 침투해 들어가기까지의 과정은 기존의 사이버 공격과 유사하지만, 최종적으로 Programmable Logic Controller (PLC)를 조작하여 원심분리기의 회전수를 증폭시킴으로써 과부하를 유도, 물리적 손상을 야기하였다 [18]. 두 번째 주목할 점은 Stuxnet이 이란 핵시설 내부로 침투하는 과정이다. 이란의 핵시설은 인터넷망 등 외부 네트워크와는 단절되어있었으나, Stuxnet은 이러한 단절 구간 (Air gap)을 통과하여 핵시설 내부로 침투하였다. 완벽하게 밝혀진 바는 아니지만 일반적으로 Stuxnet은 USB 메모리 스틱을 통하여 네트워크 단절 구간을 통과한 것으로 여겨진다[19].

Stuxnet의 사례로 볼 수 있듯, CPS에 대한 사이버 공격이 Enterprise 네트워크와 가장 두드러지게 차이나는 점은 피해의 유형과 네트워크 단절 구간의 유무이다. 물리 시스템과 사이버 시스템이 긴밀하게 연결된 CPS 특성상, 이를 대상으로 하는 공격자는 기밀성, 가용성, 무결성의 침해와 더불어 물리 공간에서의 장비와 인명 손상을 야기하는것을 목표로 할 수 있다. 한편, 많은 CPS가 외부 네트워크와 연결되지 않고 독립적인 네트워크를 구성하고 있다. 따라서 CPS에 공격을 수행하고자 하는 해커는 이러한 단절 구간을 뚫고 내부 네트워크로 침입하여야 한다.

IV. Attack Graph researches for CPS

CPS 환경에 대한 현실적인 공격 그래프를 생성하고 적절한 보안 대책을 수립하기 위해서는, 3장에서 언급했던 CPS의 두드러진 특성을 적절하게 모델링하여야 한다. CPS 환경에서의 사이버 공격은 Actuator (작동/구동기)의 오작동을 일으켜 Actuator 스스로와 그 주변 시설, 인명의 손상을 불러올 수 있다. 따라서 공격 그래프 생성을 위해 CPS 환경을 모델링하는 경우, 사이버 시스템과 Actuator 사이의 관계, 그리고 Actuator의 동작을 잘 표현할 수 있도록 모델링하여야 한다. 물리 시스템에 대한 모델링이 미흡한 경우 Actuator의 오작동으로 인한 피해를 적절하게 판단하기 어렵기 때문이다.

또 외부 네트워크와 단절된 경우가 많은 CPS 특성 상 공격자의 침투 경로를 모델링할 때 이러한 단절 구간을 극복하는 과정을 고려하여야 한다. MITRE ATT&CK for ICS 프레임워크[20]에서는 T0847 Replication Through Removable Media나 T0860 Wireless Compromise 등

공격자가 단절 구간을 극복하기 위한 공격기법(Technique)을 정의해두고 있어 이를 활용하는 것도 방법이 될 수 있다. 하지만 MITRE ATT&CK 프레임워크의 공격기법은 비슷한 범주의 공격 행위를 일반화한 것으로, 특정 시스템에서 단절 구간을 뚫고 침투하기 위한 공격 표면과 이에 대한 공격 방법을 특정하기 위해서는 추가적인 분석이 필요하다.

본 논문에서는 위에서 언급한 두 가지 관점, 즉 물리 시스템에 대한 모델링과 단절 구간에 대한 고려 여부에 초점을 맞추어 선정한 논문들을 분석하였다.

1. The aspect of modelling physical system

조사 대상 문헌 중, 물리 시스템의 동작을 모델링하여 공격 그래프 생성 또는 평가에 사용한 논문은 총 9편이었다. 이 섹션에 속한 논문들은 단절 구간에 대한 고려는 없었으나, 가능한 공격 그래프 생성의 목적에 맞도록 물리 시스템을 모델링하고자 노력하였다.

Tianlei 등은[21] 전력 시스템을 사이버 시스템과 전력 네트워크의 두 개 층으로 표현하고, 둘 사이의 관계와 전력 네트워크의 노드 사이 관계를 통하여 전력 시스템에서 발생하는 장애가 전파되는 과정을 모델링하였다. 이 논문에서 사이버 공격은 시스템 내부에서부터 시작된다.

Hasan 등은[22] 에너지 전송 시스템에 대해 MulVAL 프레임워크 기반의 공격 그래프를 생성하였고, 전력 흐름이 분기되는 부하의 값, 손상된 시스템에 의한 부하 손실을 통해 물리 시스템에 대한 피해 정도를 나타냈다. 이 연구는 인터넷망에 연결되어 있는 시스템에서 사용자가 웹 브라우저를 통해 악성 파일을 다운로드 받는 시나리오를 가정하였다.

Meyur는[23] 발전소 시스템에 대한 베이지안 공격 그래프를 생성하였는데, 물리 시스템에 대한 피해는 사이버 시스템에서 발생하는 각 우발상황에 대하여 동적 시뮬레이션을 수행함으로써 물리 시스템에 대한 피해를 측정하였다. 이때 시뮬레이션에는 변전소의 주파수와 전압 값이 사용된다. 이 논문 또한 시스템이 외부망과 연결되어 있고, 공격자가 이 망 연결성을 통해 침투하는 상황을 모델링하였다.

Castiglione과 Lupu는[24] 통신 기반 열차 제어시스템에서, 열차 사이의 간격을 물리 시스템 피해에 대한 평가 메트릭으로 사용하였다. 이는 열차 간 충돌을 야기하는 공격을 모델링한 것이며, 시스템에 대한 White Box 지식을 갖춘 공격자가 시스템 내부에 침입해 있는 상황을 가정하여 시나리오를 구성하였다. 공격 그래프 생성에는 MulVAL 프레임워크를 사용하였다.

Bhattacharya 등은[25] 공조 시스템을 대상으로 마르코프 결정 프로세스(Markov Decision Process, MDP) 기반의 공격 그래프를 생성하였으며, 시간별 온도 변화, 그리고 적정 온도와 현재 온도 사이의 간격을 사용하여 사이버 공격으로 인한 물리 시스템 피해를 평가하였다. 해당 논문도 마찬가지로 시스템이 인터넷과 연결되어 있다고 가정하였다.

Khaled 등은[26] 급수 시스템과 하수 방류 시스템에 대한 MDP 공격 그래프를 생성하였다. 건물 내 급수탱크 수위(水位)를 물리시스템 평가 지표로 사용했으며, 시스템 내부 관리자를 공격자로 설정하였다.

Semertzis 등[27]은 디지털 변전소에 대한 공격 그래프를 생성하기 위하여 MAL (Meta Attack Language) 기반의 도메인 특화 언어(Domain Specific Language, DSL)인 Substation-Lang을 제작하였다. 저자들은 다중 협응 보호체계를 모델링하여 발전기 제어 시스템 요소 차단으로 인한 점진적 장애를 모델링하였으며, 변전소 간 장거리 네트워크 구간(WAN)에 접속이 가능한 공격자를 가정하여 공격을 시뮬레이션하였다.

Zhang 등[28]은 CPS에 대한 불법적인 제어신호(illegal control signal)를 주입하여 물리 시스템 구조의 변화를 초래하는 공격을 모델링하였다. 이 연구의 특징적인 부분은 사이버 공격 시간이 누적되어 발생하는 물리 시스템 구조의 누적 편차를 사용하여 잠재적인 자산 손실을 평가하였다는 점이다. 이 연구에서는 베이지안 공격 그래프를 통해 공격 경로를 모델링하였는데, 해당 시스템이 인터넷에 연결된 상태에서 인터넷을 통하여 공격자가 시스템에 침투하는 상황을 가정하였다.

Haque 등은[29] MulVAL 프레임워크를 기반으로 생성된 공격 그래프에 대하여 공격이 시스템 임무에 미치는 영향을 평가하는 MIIAM (Mission Impact Integration and Assessment Model)을 제안하였다. 이 논문에서는 시스템 운영 문서를 활용하여 특정한 물리 시스템과 해당 물리 시스템이 수행하는 임무를 정의하였다.

2. The aspect of air gap

본 논문에서 조사한 대상 논문 중 단절 구간을 고려하여 공격 그래프 평가에 사용한 논문은 1편이었다. Buczkowski 등[30]의 연구는 CPS, IoT 등 다양한 시스템에 대한 공격 그래프를 생성할 수 있는 도구인 CySecTool을 제시하였는데, 개별 물리 시스템에 대한 모델링은 자세하지 않다는 단점이 있으나 대상 시스템에 적

용되는 USB 사용 정책을 모델링함으로써 단절 구간을 공격 그래프에 나타내고자 하였던 점은 주목할 만하다.

3. Studies which do not deal with the two aspects

Ghazo 등은[31] 모델 체커 기반의 공격그래프 생성 및 시각화 도구인 A2G2V를 제안하였다. 해당 논문은 도구의 Use case로 수질 정화시스템에 대한 사이버 공격을 모델링하였는데, Remote Code Execution이나 User Credential Construction과 같은 사이버 시스템에서의 공격기법들이 사용되었다.

Xie 등은[32] 발전소 산업제어시스템에 대하여 베이지안 공격 그래프 기반의 동적 위험 평가를 제안하였다. 그리고 실험에서는 수동적(Passive) 공격자와 능동적(Active) 공격자에 대하여 분석을 수행하였다.

Choi 등은[33] MITRE ATT&CK for ICS[34]의 Tactics와 Techniques를 기반으로 다양한 공격 시퀀스를 생성하는 방법을 제안하였다. 저자들은 사이버 공격을 일련의 Techniques 실행이라고 정의하고, Tactics가 은닉 상태(Hidden state), Techniques는 관측결과(Observation)인 은닉 마르코프 모형(Hidden Markov Model, HMM)으로 모델링하였다. 해당 논문에서는 Tactics간의 전이 관계는 MITRE ATT&CK에서 정의 된 순서인 Initial Access 부터 Impact 순서로 선형적인 전이 관계를 보이며, 각 Techniques는 해당하는 Tactics로부터 특정한 확률로 발생하는 것으로 가정하였다.

Kern 등[35]은 차량 시스템에 대한 사이버보안 평가를 위하여 모델 기반 공격 트리를 생성하는 방법을 제안하였다. 저자들은 차량 시스템을 논리 함수, 하드웨어 네트워크 아키텍처, 데이터 종속성의 집합으로 모델링하였다. 피해 시나리오에 지정된 위협원(Threat agent)으로부터 시스템 요소들 간의 연결 관계를 통해 해당 위협원이 도달할 수 있는 경로를 도출했다.

Ling 등은[36] IEC61850에 정의된 시스템 설명 구성 언어(System description Configuration Language, SCL)와 MAL[37]을 기반으로 한 공격 그래프 생성 언어인 SCL-Lang을 제안하였으며, 이를 기반으로 변전소 시스템에 대한 공격 그래프를 생성하였다. 위협 시나리오는 MITRE ATT&CK for ICS의 Tactics를 기준으로 모델링하였다.

Gressl 등[38]은 CPS 환경에서 각 장치들이 가지는 보안 제약조건을 베이지안 공격 그래프로 표현하고, 이를 시스템 디자이너가 사용하는 Design Space Exploration (DSE) 프레임워크와 통합하고자 하였다. 공격 그래프에서 각 공격행위는 STRIDE 위협 모델에 기반하여 정의되었다.

Hou 등[39]은 Internet of Vehicle (IoV) 시스템의 보안 요소와 보안 요소 사이의 관계를 모델링하기 위한 온톨로지 모델을 제안하였으며, 토폴로지가 변화하는 IoV 환경에서 동적 공격그래프 생성 알고리즘을 제안하였다. 공격 그래프 생성에는 HermiT 엔진[40]을 사용하였으며 Semantic Web Rule Language (SWRL)[41] 기반의 추론 규칙을 통해 IoV 네트워크에서 차량의 움직임에 따른 토폴로지 및 연결성 변화에 따른 공격그래프를 업데이트하였다.

Li 등[42]은 CPS에 대한 하이브리드 공격 그래프를 생성하고 이를 이용한 보안 분석 방법을 제안하였다. 시스템의 자산 속성(quality), 자산 간의 관계를 모델링하였으며 사전/사후조건(pre/post condition)에 기반한 Exploit 패턴을 정의하였다. 또 공격 그래프를 생성에 병렬 프로그래밍 구현을 통해 공격 그래프 생성속도를 향상시키고자 하였다. 공격 그래프 평가 메트릭으로는 Centrality를 사용하였다.

Ling 등[43]은 파워그리드(Power grid) SCADA 시스템에 대한 침투 테스트(Penetration test)와 위협 모델링의 결합을 시도하였다. 파워그리드 시스템의 원격 단말에 대한 침투 테스트를 수행하여 취약점들을 식별하고, 해당 취약점을 이용한 시나리오를 활용하여 MAL 기반의 DSL인 icsLang를 통해 공격 그래프를 생성하였다.

Ge 등[44]의 논문은 시스템 불연속 정보와 연속 정보를 동시에 표현할 수 있는 하이브리드 공격 그래프를 제안하고, 해당 공격 그래프를 기반으로 모델 체커 Timed Automata Checker (TACK)을 사용했다.

위의 논문들은 각 논문에서 제안한 접근법 또는 도구를 활용하여 CPS 환경에 대한 공격 그래프를 생성하는 것을 Use case로 제시하고 있으나, 물리 시스템이나 단절 구간에 대한 모델링은 결여된 한계가 있어 Enterprise 네트워크에 대한 공격 그래프 연구와 차별화되었다고 보기는 어렵다.

V. Critiques on the Identified Papers

Table 1. Classification of target papers

Modelling on physical system	[21], [22], [23], [24], [25], [26], [27], [28], [29]
Air gap	[30]
Do not deal with two aspects	[31], [32], [33], [35], [36], [38], [39], [42], [43], [44]

Table 1. 은 앞서 리뷰한 논문들을 본 논문의 초점에 맞게 분류한 것이다. 조사한 20편의 논문 중 절반인 10편은 CPS 환경에서의 공격 그래프 분석을 다루고 있으나, 사이버 시스템과 물리 시스템 사이의 관계나 물리 시스템이 현실 세계에 미치는 영향, 단절 구간을 고려하지 않는다는 점에서 기존의 Enterprise 환경에서의 공격 그래프 연구와 크게 차별점을 갖고 있다고 보기는 어렵다.

물리 시스템을 모델링하고 이에 대하여 나름의 평가 메트릭을 제안한 논문은 총 9편이며, 이 중 4편이 전력 시스템에 대한 공격 그래프를 다루고 있다. 각 연구들은 대상하는 시스템과 저자들이 설정한 시나리오에 따라 물리 시스템 피해를 정량화하는 메트릭이 모두 다르다. Tianlei 등의 연구와[21] Hasan 등의 연구[22]가 다소 유사하게 전력 시스템의 과부하 분기를 메트릭으로 사용하고 있으나, 측정기준이나 방식은 상이하다. 또 논문들에서 제시하는 물리 시스템 평가 메트릭은 보안 담당자가 해당하는 물리 시스템에 대하여 일정 수준 이상 이해하고 있지 않으면 설계가 어렵다는 단점이 있다.

한편, Buczkowski 등의 연구는[30] 범용적인 공격 그래프 생성 툴을 제안하는 논문으로 특정 물리 시스템에 대한 모델링이 제한될 수밖에 없는 한계점이 있으나, 조사한 논문 중에서는 시스템의 USB 제한 정책을 단계별로 나누는 것을 통해 단절 구간에 대한 모델링을 유일하게 시도하고 있다. 다른 연구들에서는 네트워크 단절 구간을 고려하지 않고, 시스템이 인터넷과 연결되어 있다고 가정하거나 공격자가 네트워크의 어느 한 구간에 이미 침투해있는 상황을 가정한다. 이러한 가정은, 실제로 많은 CPS 인프라가 인터넷 환경과 단절되어 있다는 현실을 반영하지 못하고 있다는 점에서 한계가 있다.

VI. Limitation of Attack Graph researches for CPS environment

Enterprise 네트워크에 대한 피해는 CVE/CVSS나 CWE/CWSS와 같이 취약점에 대한 Score를 제공하는 사이버 위협 인텔리전스 (Cyber Threat Intelligence, CTI)를 참조하여 어느 정도 객관적으로 정량화하기가 상대적으로 용이하다. 하지만 CPS 환경에서는 지금까지 물리 시스템에 대한 피해 정도를 정량화한 CTI가 부족한 실정으로 시스템 관리자나 연구자가 직접 메트릭을 설계해야 한다. 더욱이 물리 시스템의 피해에 관한 사실적인 모델링을 하기 위해서는 물리 시스템 및 기타 분야 전문가의 전문지식이 필요하다는 한계가 존재한다.

게다가, 5장에서 언급했던 것처럼, CPS 범주에 속하는 시스템들이라고 하더라도 시스템마다 그 구조, 영향 받는 위협과 이로 인한 피해가 상이하다. 따라서 모든 유형의 시스템에 대한 위협을 정량화한 CTI가 단시일에 만들어질 것으로 기대할 수는 없으며, 그러한 CTI가 제공된다고 하더라도 이를 모든 시스템에 동일하게 적용하는 것 또한 어려울 것이다.

CPS에 대한 위협을 정량화하는 데 있어 또 다른 장해요소는 적지 않은 CPS가 국가 주요 기간시설이라는 점이다[45-46]. 따라서 해당 시스템들에 대한 상세한 정보가 공개되어있지 않은 경우가 많아 위협 정량화를 위한 데이터베이스를 쌓거나 위협을 모델링하는 것은 쉽지 않다. 실제로 본 논문에서 조사한 논문들 또한 단순한 구조의 모의 CPS를 대상으로 공격 그래프를 생성하고 분석한 경우가 대부분이었다.

한편 사실적인 단절 구간 모델링도 어려운 과제다. 5장에서 알 수 있듯 대다수의 CPS 보안 분석 연구는 단절 구간이 존재하지 않는 것으로 가정하거나, 혹은 이미 단절 구간을 공격자가 통과했다는 전제하에 그 이후의 상황을 다룬다.

VII. Future research direction

CPS는 물리 시스템과 사이버 시스템이 연결되어 있다는 특징으로 인해 시스템마다 위협을 정량화하는 방법이 상이할 수밖에 없으며, 물리 시스템에 대한 피해를 모델링하는데에는 많은 도메인 지식(Domain knowledge)이 필요하다. 그러나 많은 CPS 시스템들에 대한 정보는 보안상의 이유로 공개되어있지 않으므로, 그러한 대상에 관한 학술적 연구가 수행되기는 어려운 실정이다. 따라서 앞으로의 CPS 환경에서의 공격 그래프 연구는, Automotive 등 공개된 상용 시스템에 관하여 주로 연구되거나 혹은 특정한 국가시설에 대한 보안 분석을 위한 국가 주도의 연구가 이루어질 것으로 보인다.

한편, 현재까지 많은 CPS 대상 공격 그래프 연구는 네트워크 단절 구간에 대한 모델링을 다루고 있지 않다. 그러나 네트워크 단절 구간의 존재는 CPS가 Enterprise, Cloud와 같은 다른 시스템과 구분되는 주요한 특징 중 하나이므로 사실적인 네트워크 단절 구간 모델링에 관한 연구가 수행되어야 한다.

CVSS의 temporal metric과 environmental metric

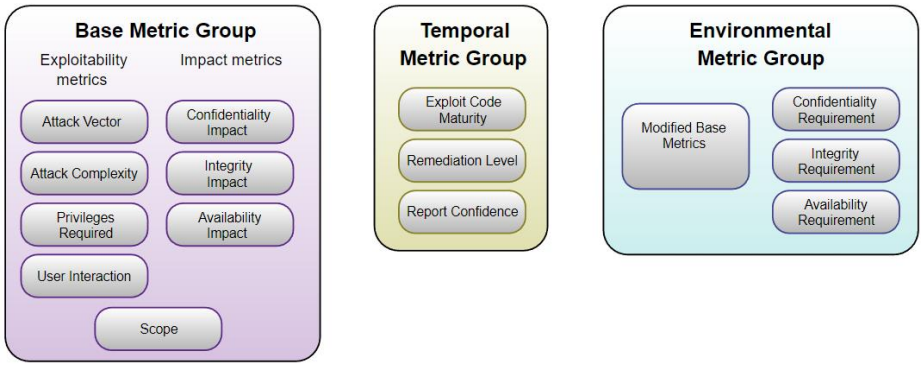

Fig. 2. CVSS Metric Groups[47]

을 적극적으로 활용하는 것도 하나의 방법이 될 수 있다. 많은 공격 그래프 연구들이 취약점의 위험도를 판단할 때 자산에 존재하는 CVE에 대하여 CVSS score 누적 합(weighted sum)을 사용하는데, 많은 경우 base metric에 대한 평가만을 사용한 base score를 이용한다. 하지만 temporal metric과 environmental metric에는 CVE에 대한 exploit 코드의 기 존재 여부를 나타내는 공격 코드 성숙도 (Exploit Code Maturity), 대상 시스템에서 가용성 침해가 얼마나 치명적인지를 나타내는 가용성 요구도 (Availability Requirement) 등 CPS 환경에 적용할 만한 요소들이 일부 존재한다. 이러한 요소들을 통해 CVSS score의 가중합을 보다 현실적으로 보정할 수 있다. Fig. 2.는 CVSS Metric 그룹과 각 그룹에 포함된 평가 요소를 나타낸다.

VIII. Conclusions

Lazarus[48], Kimsuky[49], Sandworm[50] 등 국가지원 해킹그룹 (State-sponsored)들은 전력 시스템 등의 CPS를 공격해 오고 있으며, 우크라이나 사이버전의 사례[51]로 알 수 있듯 CPS에 대한 위협은 증가하고 있다. 보안 정책을 망 분리 환경에 의지하여 내부망 보안을 취약하게 관리하는 경우 USB 유입, Spearphishing 등의 이유로 인해 사이버 공격이 발생하였을 때 심각한 재난으로까지 이어질 수 있는데, 이러한 위협들에 대하여 현실적인 모델링을 할 수 있는 도구가 필요하다.

공격자의 침투 경로를 모델링하고 위협을 분석하기 위한 방법론인 공격 그래프는 주로 Enterprise 네트워크를 대상으로 연구되었으며, 현재는 CPS, Cloud, IoT 등 다양한 분야에 공격 그래프를 적용하고자 하는 시도가 이루어지고 있다. 본 논문에서는 최근 5년간 가장 많은 연구 비중을 차지하고 있는 CPS 환경에서의 공격 그래프 연구를 조사하였다.

조사 된 연구 중 절반은 CPS의 특징적인 두 요소 (물리 시스템과 단절 구간 모델링)를 고려하지 않아 Enterprise 네트워크에 관한 연구와 특별한 차이를 보이지 않았다. 또, 일부 연구들은 물리 시스템 혹은 단절 구간을 모델링하려는 시도를 하였으나, 정보가 공개되어있지 않은 경우가 많은 CPS의 특성과 네트워크 단절 구간을 현실적으로 모델링하기 어렵다는 점으로 인하여 지금까지의 CPS 환경을 대상으로 한 공격 그래프 연구에는 한계가 존재한다.

이러한 한계를 토대로, 본 논문에서는 앞으로 CPS 환경 대상 공격 그래프에 관한 연구가 나아갈 두 가지 방향을 제시하였다. 앞으로는 공개된 CPS 환경에 관한 연구가 주를 이룰 것으로 보는 것이 현실적이며, 기반 시설 등에 관한 연구는 국가 주도로 이루어질 것이다. 또, 네트워크가 단절된 CPS를 분석하기 위하여 단절 구간을 모델링하는 방법에 관한 연구가 수행되어야 한다.

REFERENCES

[1] Phillips, Cynthia, and Laura Painton Swiler. "A graph-based system for network-vulnerability analysis." Proceedings of the 1998 workshop on New security paradigms. 1998. pp. 71-79, January 1998. DOI: 10.1145/310889.310919

[2] Jha, Sheyner, and Wing. "Two formal analyses of attack graphs." Proceedings 15th IEEE Computer Security Foundations Workshop. 2002. pp. 49-63, June 2002. DOI: 10.1109/CSFW.2002.1021806

[3] Sheyner, Haines, Jha, Lippmann, and Wing. "Automated generation and analysis of attack graphs." Proceedings 2002 IEEE Symposium on Security and Privacy. 2002. pp. 273-284, May 2002. DOI: 10.1109/SECPRI.2002.1004377

[4] Ou, Xinming, Govindavajhala, and Appel. "MulVAL: A Logic-based Network Security Analyzer." Proceedings of the 14th conference on USENIX Security Symposium - Volume 14. 2005.

pp. 8, July 2005. DOI: 10.5555/1251398.1251406

[5] Hong and Kim, "HARMS: Hierachical Attack Representation Models for Network Security Analysis." Proceedings of the 10th Australian Information Security Management Conference. 2012. December 2012. DOI: 10.4225/75/57b559a3cd8da

[6] Kaynar and Sivrikaya, "Distributed Attack Graph Generation." Distributed Attack Graph Generation, vol 13, 2015. pp. 519-532. April 2015. DOI: 10.1109/TDSC.2015.2423682

[7] Hong, Kim, Chung, and Huang. "A survey on the usability and practical applications of Graphical Security Models." Computer Science Review. vol.26. 2017. pp. 1-16, October 2017. DOI: 10.1016/j.cosrev.2017.09.001

[8] Frigault and Wang, “Measuring Network Security Using Bayesian Network-Based Attack Graphs” 32nd Annual IEEE International Computer Software and Applications Conference, August 2008. DOI: 10.1109/COMPSAC.2008.88

[9] Joy, Jahan, Kabir and Mahato, “Precise Estimation of Local Probabilities for Bayesian Attack Graph Analysis” IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference, October 2021. DOI: 10.1109/IEMCON53756.2021.9623254

[10] Gallon and Bascou, "CVSS Attack Graphs." 2011 Seventh International Conference on Signal Image Technology & Internet-Based Systems, 2011. January 2012. DOI: 10.1109/SITIS.2011.24

[11] Keramati, Akbari and Keramati, "CVSS-based security metrics for quantitative analysis of attack graphs." International eConference on Computer and Knowledge Engineering, 2013. December 2013. DOI: 10.1109/ICCKE.2013.6682816

[12] Lu et al., "Ranking Attack Graphs with Graph Neural Networks." Proceedings of the 5th International Conference on Information Security Practice and Experience, 2009. pp. 345-359. April 2009. DOI: 10.1007/978-3-642-00843-6_30

[13] Clarivate, Web of Science, https://www.webofknowledge.com/

[14] Association for Computing Machinary, ACM Digital Library, https://dl.acm.org/

[15] Institute of Electrical and Electronics Engineers, IEEE Xplore, https://ieeexplore.ieee.org/

[16] UC Berkeley (EECS Dept.), Ptolemy project, https://ptolemy.berkeley.edu/projects/cps/

[17] Kushner, David, “The real story of stuxnet” IEEE Spectrum, Volume 50, Issue 3. March 2013. pp. 48-53. DOI: 10.1109/MSPEC.2013.6471059

[18] Kesler, Brent, “The vulnerability of nuclear facilities to cyber attack” Strategic Insights, Volume 10, Issue 15. 2011.

[19] Kopfstein, “Stuxnet virus was planted by Israeli agents using USB sticks, according to new report”, The Verge, https://www.theverge.com/2012/4/12/2944329/stuxnet-computer-virus-planted-israeli-agent-iran

[20] MITRE, MITRE ATT&CK for ICS, https://attack.mitre.org/tactics/ics/

[21] Tianlei, Shibin, Baoxu, Tao and Tao. "Integrated fault propagation model based vulnerability assessment of the electrical cyber-physical system under cyber attacks". Reliability Engineering & System Safety, Volume 189, pp. 232-241, September 2019, DOI: 10.1016/j.ress.2019.04.024

[22] Hasan, Shetty, Hassanzadeh and Ullah, “Towards Optimal Cyber Defense Remediation in Cyber Physical Systems by Balancing Operational Resilience and Strategic Risk”. 2019 IEEE Military Communications Conference, November 2019, DOI: 10.1109/MILCOM47813.2019.9021076

[23] Meyur, "A Bayesian Attack Tree Based Approach to Assess Cyber-Physical Security of Power System", 2020 IEEE Texas Power and Energy Conference (TPEC), February 2020, DOI: 10.1109/TPEC48276.2020.9042529

[24] Castiglione and Lupu, "hazard driven threat modelling for cyber physical systems". CPSIOTSEC'20: Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy. November 2020. pp. 13-24. DOI: 10.1145/3411498.3419967

[25] Bhattacharya, Ramachandran, Banik, Dowling and Bopardikar. "Automated Adversary Emulation for Cyber-Physical Systems via Reinforcement Learning". 2020 IEEE International Conference on Intelligence and Security Informatics, November 2020, DOI: 10.1109/ISI49825.2020.9280521

[26] Khaled, Ouchani, Tari and Drira, "Assessing the Severity of Smart Attacks in Industrial Cyber-Physical Systems". ACM Transactions on Cyber-Physical Systems, Volume 5, Issue 1. December 2020. pp 1–28. DOI: 10.1145/3422369

[27] Semertzis, Rajkumar, Stefanov, Fransen and Palensky, "Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs." 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES). May 2022. DOI: 10.1109/MSCPES55116.2022.9770140

[28] Zhang, Li, Zou and Niu, "Quantitatively Assessing the Cyber-to-Physical Risk of Industrial Cyber-Physical Systems." Proceedings of the 2020 on Great Lakes Symposium on VLSI. September 2020. pp. 439–444. DOI: 10.1145/3386263.3406945

[29] Haque, Shetty, Kamhoua and Gold, “Integrating Mission-Centric Impact Assessment to Operational Resiliency in Cyber-Physical Systems”. 2020 IEEE Global Communications Conference, December 2020, DOI: 10.1109/GLOBECOM42002.2020.9322321

[30] Buczkowski, Malacaria, Hankin and Fielder, "Optimal Security Hardening over a Probabilistic Attack Graph: A Case Study of an Industrial Control System using CySecTool." Sat-CPS '22: Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems. April 2022. pp. 21-30. DOI: 10.1145/3510547.3517919

[31] Ghazo, Ibrahim, Ren and Kumar, "A2G2V: Automatic Attack

Graph Generation and Visualization and Its Applications to Computer and SCADA Networks". IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 10, pp. 3488-3498, October 2020, DOI: 10.1109/TSMC.2019.2915940.

[32] Xie, Jianbo, Keda SUN, and Xubing LEI. "Risk assessment method of power plant industrial control information security based on Bayesian attack graph". Journal of Electrical Systems, Volume 17, Issue 4, pp. 529-541, 2021

[33] Choi, Yun and Min, "Probabilistic Attack Sequence Generation and Execution Based on MITRE ATT&CK for ICS Datasets." CSET '21: Cyber Security Experimentation and Test Workshop. August 2021. DOI: 10.1145/3474718.3474722

[34] MITRE, ATT&CK, https://attack.mitre.org/

[35] Kern, Liu, Betancourt and Becker, "Model-based Attack Tree Generation for Cybersecurity Risk-Assessments in Automotive." 2021 IEEE International Symposium on Systems Engineering (ISSE). October 2021. DOI: 10.1109/ISSE51541.2021.9582462

[36] Ling and Ekstedt, "Generating Threat Models and Attack Graphs based on the IEC 61850 System Configuration description Language." SAT-CPS '21: Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems. April 2021. pp. 98-103. DOI: 10.1145/3445969.3450421

[37] Foreseeti AB, MAL, https://mal-lang.org/

[38] Gressl, Steger and Neffe, "Design Space Exploration for Secure IoT Devices and Cyber-Physical Systems." ACM Transactions on Embedded Computing Systems, Volume 20, Issue 4. May 2021. pp. 1-24. DOI: 10.1145/3430372

[39] Hou, Chen, Ma, Zhou and Yu, "An Ontology-Based Dynamic Attack Graph Generation Approach for the Internet of Vehicles." Frontiers in Energy Research, June 2022, Volume 10. DOI: 10.3389/fenrg.2022.928919

[40] Glimm, Horrocks, Motik, Stoilos and Wang. "HermiT: An OWL 2 Reasoner." Journal of Automated Reasoning, 53. May 2014. pp. 245-269. DOI: 10.1007/s10817-014-9305-1

[41] Horrocks, Patel-Schneider, Boley, Tabet, Grosof and Dean, "SWRL: A Semantic Web Rule Language Combining OWL and RuleML." W3C Member submission Volume 21 Issue 79. May 2004. pp. 1-31. DOI: -

[42] Li, Hawrylak and Hale, "Strategies for Practical Hybrid Attack Graph Generation and Analysis." Digital Threats: Research and Practice, Volume 3, Issue 4. May 2022. pp. 1-24. DOI: 10.1145/3491257

[43] Ling, Cabus, Butun, Lagerström and Olegrad, "Securing Communication and Identifying Threats in RTUs: A Vulnerability Analysis." ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security. August 2022. pp. 1-7. DOI: 10.1145/3538969.3544483

[44] Ge, Shen, Xu and He, "A Hybrid Attack Graph Analysis Method based on Model Checking." 2022 Tenth International Conference on Advanced Cloud and Big Data (CBD). November 2022. DOI: 10.1109/CBD58033.2022.00053

[45] CISA, Critical Infrastructure Sectors, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[46] Ministry of the Interior and Safety, Protect Nation Core Foundation, https://www.mois.go.kr/frt/sub/a06/b13/protectNationCoreFoundation/screen.do

[47] FIRST, Common Vulnerability Scoring System v3.1:Specification Document, https://www.first.org/cvss/v3.1/specification-document

[48] MITRE, Lazarus Group, https://attack.mitre.org/groups/G0032/

[49] MITRE, Kimsuky, https://attack.mitre.org/groups/G0094/

[50] MITRE, Sandworm Team, https://attack.mitre.org/groups/G0034/

[51] Bing, "Russian hackers preparing new cyber assault against Ukraine-Microsoft report", Reuters, https://www.reuters.com/technology/russian-hackers-preparing-new-cyber-assault-against-ukraine-microsoft-report-2023-03-15/

Authors

Junho Jang received his B.S. degree in Computer Science from Korean Air Force Academy in 2013. He is currently pursuing Ph.D degree in Cybersecurity at Korea University. He is currently a commissioned officer in Korean Air Force. His research interest is in Data-driven security, Threat modelling, Adversary automatisation, and Vehicle security.

Saehee Jun received a B.S. degree in information security from Seoul Women's University in 2020. She is currently enrolled on the M.S. course in Cybersecurity at Korea University. She is interested in Automotive Security, data-driven security, AI Security, Anomaly Detection.

Huiju Lee received her B.S. degree in Management Information Systems, Convergence Security from Korea University (Sejong campus) in 2022. She is currently a M.S. student in the School of Cybersecurity at Korea University. She is interested in Data-driven Security, Anomaly Detection, Cyber Threat Intelligence.

Jaegwan Yu received his M.S degrees in security Engineering from Sungkyunkwan University in 2017. He is currently a research engineer in LIGNex1. He is interested in Adversary automation, Cyber-warfare Training and Anti-Tamper.

Sungjin Park received his B.S. degree in Cyber Security from Ajou University in 2020. he is currently a research engineer in LIGNex1. He is interested in Cyber Threat Intelligence, AI Security and Offensive Security.

Su-Youn Hong received her Ph. D degrees in electrical engineering from KAIST, Korea in 2013. She is currently a chief research engineer in LIGNex1. She is interested in Threat and defense procedure modeling, Adversary automation and Cyber-warfare Training.

Huy Kang Kim received his B.S. degree in Industrial Management in 1998, M.S. and Ph.D degrees in industrial and systems engineering from KAIST in 2000 and 2009. He founded A3 Security Consulting, the first information security consulting company in Korea in 1999. Currently he is an associate professor in Graduate School of Information Security, Korea University. Before joining Korea University, he was a technical director (TD) and a head of information security department of NCSOFT (2004~2010). His research interests include solving security problems in online games based on the user behavior analysis and data mining.