*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.31, NO.5, Oct. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.5.1021

# 사이버 공격 훈련 시나리오 표현을 위한 Stage 기반 플로우 그래프 모델 연구*

김 문 선,[1†] 이 만 희[2‡]
[1,2]한남대학교 (대학원생, 교수)

# A study on Stage-Based Flow Graph Model for Expressing Cyber Attack Train Scenarios*

Moon-Sun Kim,[1†] Man-Hee Lee[2‡]
[1,2]Hanam University (Graduate student, Professor)

요 약

본 논문은 현대의 복잡한 사이버 공격을 모사하는 훈련 시나리오를 효과적으로 표현하기 위한 모델인 S-CAFG(Stage-based Cyber Attack Flow Graph)를 제안하고 평가한다. 이 모델은 더 복잡한 시나리오 표현을 위해 기존 그래프 및 트리 모델을 결합하고 stage 노드를 도입했다. 평가는 기존 모델링 기법으로는 표현하기 어려운 시나리오를 제작하고 이를 S-CAFG로 모델링하는 방식으로 진행했다. 평가 결과, S-CAFG는 동시 공격, 부가적 공격, 우회 경로 선택 등 매우 복잡한 공격 시나리오를 효과적으로 표현할 수 있음을 확인했다.

ABSTRACT

This paper proposes S-CAFG(Stage-based Cyber Attack Flow Graph), a model for effectively describing training scenarios that simulate modern complex cyber attacks. On top of existing graph and tree models, we add a stage node to model more complex scenarios. In order to evaluate the proposed model, we create a complicated scenario and compare how the previous models and S-CAFG express the scenario. As a result, we confirm that S-CAFG can effectively describe various attack scenarios such as simultaneous attacks, additional attacks, and bypass path selection.

**Keywords:** Cyber attack model, Cyber range, Cyber attack scenario, network security

## I. 서 론

네트워크 기술의 발달로 인해 기업 및 기관의 많은 업무 프로세스가 사이버 공간으로 이동하고 있다. 이에 따라, 기업 및 기관의 데이터 탈취나 시스템 파괴를 목적으로 하는 사이버 공격이 급증하고 있다. 예를 들어, 데이터를 암호화한 뒤, 복호화 키를 대가로 금전을 요구하는 랜섬웨어 공격은 가장 유행하는 사이버 공격 유형 중 하나이다[1]. 이러한 사이버 공격은 기업 및 기관에 막대한 피해를 입힐 수 있기 때문에 이를 방지하는 것이 중요하다. 따라서 기업 및 기관은 방화벽 및 침입 탐지 시스템(IDS, Intrusion Detection System)을 운영하는 등 철저한 네트워크 보안 체계를 구축할 필요가 있다.

하지만 APT(Advanced Persistent Threat)과 같이 고도화되는 사이버 공격을 모두 방어할 수 있는 보안 체계를 구축하는 것은 현실적으로 불가능하다. 이에 따라 세계 각국의 기관 및 기업은 사이버

Received(08. 17. 2021), Modified(09. 13. 2021), Accepted(09. 13. 2021)
* 이 성과는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2021R1A4A2001810)
† 주저자, kmoonsun95@gmail.com
‡ 교신저자, manheelee@hnu.kr(Corresponding author)

위협에 대한 보안 담당자의 대응 능력을 향상시키기 위해 사이버 공격 대응 훈련을 진행하고 있다[2,3,4].

사이버 공격 대응 훈련은 가상 환경에 구축된 사이버 훈련장을 활용하는 경우가 많다. 가상 환경 기반 훈련장의 이점은 다양한 사이버 공격을 시뮬레이션하기 위해 네트워크의 구성 요소를 자유롭게 변경할 수 있어 환경 구축 비용이 적고 시스템 운영이 효율적이다. 다만, 사이버 훈련장을 운영하기 위해서는 고도로 훈련된 인적 자원이 필요하다. 따라서 현실적인 훈련장 운영을 위해서는 자동화된 공격 및 채점 기준인 사이버 공격 모델과 훈련 시나리오를 다양하게 구축하는 것이 필요하다[2,5,6].

사이버 공격 모델은 특정 사이버 공격이 일어나는 과정에서 발생하는 공격 기법 및 침투 경로를 표현하는 모델이다. 이러한 사이버 공격 모델링에는 주로 그래프 기반 모델과 트리 기반 모델이 사용된다. 다만, 그래프 모델은 시나리오의 규모가 클수록 표현이 복잡해지는 한계점이 있어 트리 기반 모델이 보다 널리 사용된다. 트리 기반 모델은 해커의 최종 목표인 root 노드로 향하는 leaf 노드들의 흐름을 통해 사이버 공격을 체계적으로 모델링한다[7,8].

사이버 공격 훈련 시나리오는 사이버 공격 모델을 바탕으로 공격 발생 시기와 순서, 침투 경로, 우회 공격 기법 사용 등 실제 해커의 사이버 위협 과정에서 발생할 수 있는 과정을 정밀하게 모사한다. 주로 사이버 공격의 양상을 파악하여 보안 대책을 수립하기 위해 사용되는 사이버 모델링과 달리, 사이버 공격 훈련 시나리오는 훈련자의 사이버 위협 대응 능력을 향상시키기 위한 훈련 콘텐츠로 제작되는 점에서 차이가 있다.

사이버 공격 훈련 시나리오의 모델링은 일반적으로 트리 모델이 사용된다[9,10,11,12]. 트리 모델은 시나리오의 흐름과 목적을 간략히 표현할 수 있는 장점이 있다. 하지만 최신 시나리오는 사이버 공격 과정에서 발생하는 복잡하고 다양한 정보들로 구성된다. 따라서 일반적인 트리 모델로는 시나리오를 온전히 표현하기 어려운 경우가 있다.

따라서 본 논문은 복잡한 사이버 공격 훈련 시나리오를 효과적으로 표현할 수 있는 모델링 기법인 Stage 기반 사이버 공격 흐름 그래프(S-CAFG, Stage-based Cyber Attack Flow Graph)를 제안한다. S-CAFG는 기존 모델이 표현할 수 없었던 세분화된 공격 기법 및 우회 경로를 표현하기 위해 그래프 모델과 트리 모델의 모델링 규칙을 결합했다. 또한 시나리오의 다양한 요소를 효과적으로 표현하기 위한 새로운 구성 요소인 stage 노드를 도입했다. Stage 노드는 훈련 시나리오의 특정 공격 단계 만족을 위한 하위 노드의 조건을 명시하고 다양한 분기점을 제공한다. 여기서 분기점은 해커의 변형된 공격 및 우회 경로 침투와 같은 복잡한 시나리오를 표현하는 역할을 한다.

본 논문은 S-CAFG를 평가하기 위해 복잡한 사이버 공격 훈련 시나리오를 제작하고 이 시나리오를 S-CAFG로 표현했다. 그 결과, 기존의 트리 모델이 표현하지 못했던 해커의 복잡한 공격 기법과 경로를 S-CAFG가 효과적으로 표현할 수 있는 것을 확인했다. 따라서 S-CAFG를 통해 최신 사이버 공격 훈련 시나리오를 모델링하면 보다 효과적으로 훈련 시나리오 제작 및 공격 단계별 채점 기준 마련이 가능할 것으로 판단된다.

## II. 관련 연구

### 2.1 공격 그래프 모델

공격 그래프 모델은 해커가 공격 목표에 침투할 수 있는 모든 경로를 표현하는 모델이다. 보안 관계자는 이를 통해 네트워크의 취약점을 분석하고 해커의 침투 경로를 사전에 차단할 수 있다. 이러한 그래프 모델은 크게 노드와 간선(edge)으로 구분되며, 사용되는 목적에 따라 더 다양한 요소를 가지기도 한다[13].

공격 그래프 모델은 대표적으로 dependency 기반과 시나리오 기반 공격 그래프가 있다. dependency 공격 그래프는 사이버 공격에 필요한 사전 조건, 공격 유형, 공격 성공에 따른 사후 행위들의 의존 관계를 방향 그래프를 사용하여 모델링한다. 시나리오 기반 공격 그래프는 해커의 악의적인 행위들을 시뮬레이션하고 이를 바탕으로 공격 그래프를 생성한다[14,15].

이러한 그래프 기반 모델링은 방대한 네트워크의 구성 요소를 파악하고 각 경로별 취약점을 파악할 수 있는 장점이 있다. 하지만 그래프 기반 모델링은 각 공격의 유형, 우회 경로, 공격 순서 등 복잡한 훈련 시나리오를 표현하기 위한 요소들이 부족하다. 또한 시나리오가 길거나 복잡할수록 그래프가 상당히 복잡해지는 단점이 있다. 따라서 사이버 공격 훈련 시나

리오 모델링은 주로 트리 기반 모델이 사용된다.

### 2.2 공격 트리 모델

사이버 보안 관점에서 공격 트리는 다양한 사이버 공격 표면(attack surface)을 체계적으로 모델링하여 보다 안정적인 위협 관리 및 보안 대책 수립을 위해 사용된다. 공격 트리 모델의 구조는 공격의 최종 목표인 root 노드, 공격을 나타내는 leaf 노드, 공격의 흐름을 표현하는 간선, 노드의 조건을 나타내는 속성으로 구성된다. 여기서 속성은 다음 단계로 넘어가기 위한 조건을 논리식인 AND와 OR로 표현한다[8].

Fig. 1은 공격 트리 모델의 예시를 보여준다. root 노드 $n_0$은 각 공격의 구현인 여러 개의 하위 노드를 가진다. 여기서 모든 간선은 자식 노드에서 부모 노드로 향하는 상향식 공격 진행 방향을 표현한다. 또한 각 간선은 논리적 관계를 가질 수 있다. 예를 들어, $n_1$과 $n_2$은 OR로 연결되므로 각 노드가 하나만 만족해도 상위 노드로 이동할 수 있다. 반면, $n_3$과 $n_4$은 AND 속성으로 연결되기 때문에 두 노드의 조건이 모두 만족되어야만 상위 노드로 이동할 수 있다. 정리하자면 상위 노드 N으로 도달할 수 있는 경우는 $n_1$또는 $n_2$가 만족되는 경우와 $n_3$과 $n_4$가 동시에 만족되는 경우이다.

이처럼 공격 트리 모델은 보안 위협 및 사이버 공격 절차를 간단하게 표현할 수 있지만, 사이버 공격 시나리오를 표현하기에는 한계점이 있다. 예를 들어, Fig. 1의 시나리오는 각 공격의 우선순위나 공격 시작점을 알 수 없다. 또한 실제 사이버 공격은 특정 공격 기법이 실패하는 경우, 우회 경로를 거치거나 새로운 공격 기법을 사용한다. 이러한 복잡한 시나리오를 표현하기 위해 AND와 OR 속성만으로는 한계가 있다[9,10,11]. 이에 따라 기존 트리 모델에 새로운 구성 요소를 추가하여 보다 다양한 표현을 가능하게 하는 연구들이 수행되었다.

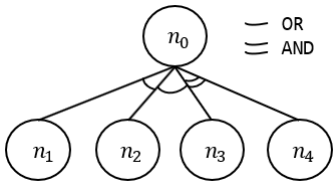



Fig. 1. Attack tree model

### 2.3 E-CAT 모델

E-CAT(Extended Cyber Attack Tree)는 네트워크 취약성 분석을 위한 사이버 공격 모델링의 한계점을 극복하기 위해 제안되었다. 이 모델은 기존의 공격 트리 모델에 새로운 요소인 CON(Condition Composition), Boolean 표현식, AGP(Attack Generation Probability)를 추가하여 기존에는 불가능했던 공격의 다양성, 공격 조건 표현, 공격 경로 선택 정보를 표현할 수 있도록 개선했다[9].

여기서 CON은 기존의 공격 방법으로 표현하기 어렵거나 변형된 공격을 나타내는 속성이다. Boolean 표현식은 기존 공격 트리의 복잡한 조건식 표현을 $\wedge$과 $\vee$으로 간략히 표현할 수 있도록 한다. AGP는 OR 조합으로 연결된 노드에서 각 노드의 공격 성공 확률을 나타낸다. 이를 통해 해커가 선택할 확률이 가장 높은 공격 경로를 예측할 수 있다.

Fig. 2는 E-CAT 모델의 예시이다. 공격 목표인 $n_0$ 의 자식 노드인 $n_1$은 $n_{1.1}$ CON $n_{1.2}$으로 연결된다. 이때 $n_{1.2}$은 정의되지 않은 예외적인 공격을 의미한다. E-CAT 모델은 이 표현을 Boolean 식을 사용하여 $n_1 = (n_{1.1} \veebar n_{1.2})$으로 간단히 표현할 수 있다. 이 식에서 $\veebar$는 CON을 의미한다.

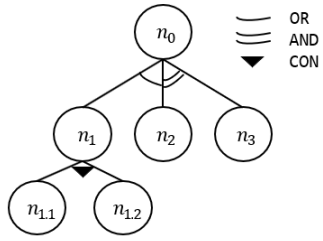



Fig. 2. E-CAT model

### 2.4 D-CAT 모델

D-CAT(Dynamic-Cyber Attack Tree)은 기존 공격 트리 모델이 공격 순서와 우선순위를 알 수 없는 점을 개선하기 위해 제안되었다. 이 모델은 트리 모델에 S_AND와 번호(label) 속성을 추가하여 공격 순서를 명확히 정의할 수 있도록 개선했다. 또

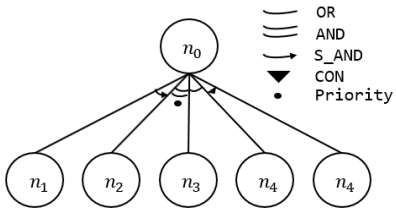



Fig. 3. D-CAT model

한 E-CAT 모델과 같이 CON 속성을 통해 복잡하고 변형된 시나리오를 표현할 수 있도록 한다[10].

Fig. 3은 D-CAT 모델의 예시이다. 첫 번째 leaf 노드 $n_1$ 은 $n_2$ 노드와 S_AND로 연결된다. 이는 $n_1$ 공격이 먼저 수행된 이후 $n_2$ 공격이 수행되는 것을 의미한다. S_AND가 없는 나머지 노드들은 노드에 부여된 번호를 바탕으로 공격 순서를 결정한다. Priority 속성은 AND로 연결된 노드에 부여될 수 있으며 가장 먼저 실행되는 공격 조합을 의미한다.

### 2.5 Adapted 공격 모델

Adapted 공격 모델은 기존 트리 모델을 표현하는 요소들의 표기법을 세분화했다. 또한 추상 노드를 도입하여 사이버 공격 시나리오를 효과적으로 표현할 수 있도록 트리 모델을 개선했다. 추상 노드는 동시에 실행되거나 순차적으로 수행되는 공격을 표현할 수 있으며, 이를 바탕으로 노드의 실행 순서 정의 및 복잡한 시나리오 표현을 가능하도록 한다[11].

Fig. 4는 Adapted 모델이 제안하는 노드 표기법을 보여준다. Actor 노드는 일반적인 공격 수행 노드를 의미한다. 이때 노드의 번호, 공격 실행 시간과 수행 시간, 공격 대상을 함께 명시하여 보다 많은 정보를 전달할 수 있도록 한다. 또한 4개의 추상 노드를 통해 순차적 공격과 동시 실행 공격을 구분할 수 있다.

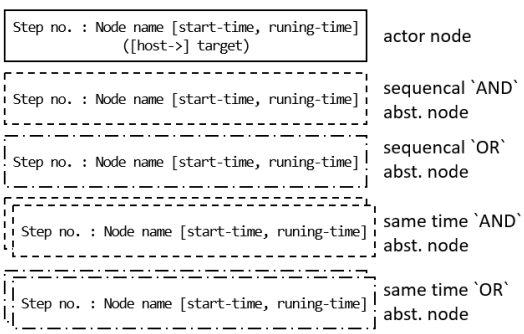



Fig. 4. Abstract nodes of adapted attack model

## III. Stage 기반 사이버 공격 흐름 그래프

본 장에서는 최신 사이버 공격 훈련 시나리오를 모델링하기 위한 새로운 기법의 필요성에 대해 설명한다. 이후 본 논문에서 제안하는 사이버 공격 훈련 시나리오 모델링 기법인 S-CAFG를 소개한다.

### 3.1 최신 공격의 복잡도와 기존 모델의 한계

E-CAT 모델과 D-CAT 모델은 기존 공격 트리 모델의 한계점을 극복하기 위해 더 다양한 속성과 표현을 추가했다. 이를 통해 기존 트리 모델이 표현하기 어려웠던 공격 순서, 중요성, 예외 이벤트 등의 표현이 가능해졌다. 하지만 최신 사이버 훈련 시나리오의 복잡한 흐름을 표현하기에는 여전히 한계점이 있다.

Fig. 5는 기존 트리 기반 모델들이 가지는 한계점을 간단한 시나리오를 통해 보여준다. 해커는 데이터베이스의 자료를 유출하기 위해 사이버 공격을 수행한다. 이를 위해서 해커는 SQL injection 공격과 관리자 세션 탈취 공격을 선택할 수 있다. 이때, SQL injection 공격은 blind 기반과 union 기반 등 매우 다양한 기법들이 사용될 수 있다. 하지만 트리 구조에서 자식 노드는 하나의 부모 노드만 갖기 때문에 기존 모델은 SQL injection 공격의 다양한 유형을 표현할 수 없다. 또한 시나리오 상에서 SQL injection과 세션 탈취는 모두 네트워크 스캐닝 공격이 선행되어야 한다. 이 또한 자식 노드가 두 개

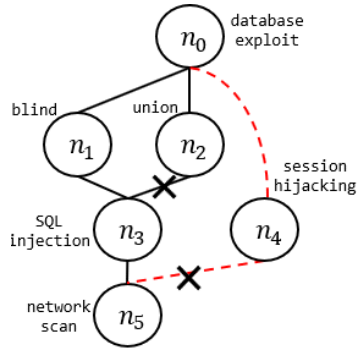



Fig. 5. Limitation of tree-based model

이상의 부모를 가지게 되므로 성립할 수 없다. 따라서 다양한 공격 유형 및 중복되는 공격 경로들을 모두 다른 노드로 표현해야 한다.

Adapted 공격 모델은 추상 노드와 점선 표기법을 바탕으로 공격 시나리오의 순차성 및 동시성을 표현한다. 하지만 시나리오가 복잡할수록 점선으로 구분된 노드의 의미를 명확히 파악하기가 어려울 수 있다. 또한 노드에 공격 시간을 명시하는 특성상 동적으로 공격 유형 및 공격 시작 시간을 선택하는 복잡한 훈련 시나리오에는 적용하기 어렵다. 따라서 해커의 다양한 공격 경로 및 유형을 모사하는 최신 사이버 공격 훈련 시나리오를 표현하기 위해서는 새로운 공격 모델링 기법이 필요하다.

## 3.2 Stage 기반 사이버 공격 흐름 그래프

본 절은 최신 사이버 공격 훈련 시나리오를 효과적으로 모델링할 수 있는 S-CAFG를 설명한다. S-CAFG는 해커의 공격 유형 및 경로 선택을 표현하기 위해 그래프 모델을 기반으로 한다. 이때 leaf 노드부터 root 노드까지의 공격 흐름을 명시하는 트리 모델의 상향식 표현 기법을 그래프 모델에 적용하여 그래프가 지나치게 복잡해지는 것을 방지한다. 또한 stage 노드를 추가하여 시나리오의 다양한 분기점과 진행 조건을 명확히 표현한다.

### 3.2.1 S-CAFG의 구성 요소

S-CAFG는 3가지 기호로 공격 시나리오를 표현한다. 이에 대한 설명은 Table 1과 같다. Actor 노드는 하나의 공격 유형 및 상태를 의미한다. 여기서 공격 단위는 TCP 스캔, command injection, packet sniffing과 같은 다양한 공격 유형이다. 또한 각 공격 유형은 여러 가지 변형된 공격으로 표현할 수도 있다. Actor 노드의 상태는 희생자의 행위나 특정 환경을 만족할 때까지 기다리는 특수한 상태를 의미한다. 각 actor 노드에 부여된 순서 번호는 시나리오의 공격 순서를 표현할 때 사용한다. 이러한 Actor 노드는 자신을 제외한 모든 노드와 연결될 수 있으며 반드시 하나 이상의 상위 노드와 연결되어야 한다.

Stage 노드는 actor 노드 및 stage 노드를 하위 노드로 가지는 분기점이다. 이는 특정 공격 단계를 성공시키기 위한 하위 노드의 조건을 명시하며,

Table 1. Symbols of S-CAFG

| symbol | name | description |
|---|---|---|
| $n_m$ | actor node | attack type and status |
| Stage [n]<br>[description]<br>stage rules | stage node | conditions for successful attack |
| ——— | edge | attack flow |

다음 단계 공격을 위한 다양한 분기점을 제공한다. 여기서 분기점은 특정 공격이 실패했을 경우, 다른 공격 기법을 사용하거나 변형된 공격을 수행하는 복잡한 시나리오 표현하는 역할을 한다. 또한 각 노드의 실행 순서 및 조건을 논리식과 기호로 간결하게 표현할 수 있는 편의성을 제공한다.

Stage 노드는 같은 stage 노드를 포함하여 여러 개의 actor 노드와 연결될 수 있다. 최상위 stage 노드는 공격의 목표지점(Goal)을 의미한다. Edge는 각 노드의 연결 관계를 나타낸다. 트리 모델과 같이 상향식 방향 그래프를 그리기 때문에 공격 흐름은 오직 하위 요소부터 상위 요소로만 향할 수 있다.

### 3.2.2 Stage 노드의 속성

Stage 노드는 4가지 속성을 통해 해커가 다음 단계 공격으로 나아가기 위해 만족해야 할 규칙들을 명시한다. 이에 대한 설명은 Table 2와 같다. ∧ 기호는 연결된 두 노드가 모두 만족해야 하는 경우를 명시한다. ∨ 기호는 연결된 노드 중 하나만 만족하면 되는 선택적인 경우를 명시한다. 〉 기호는 이어지는 노드가 stage를 만족하기 위한 필수 요소는 아니지만 해커가 추가적인 정보 획득을 위해 수행할 수 있는 부가적인 행위를 정의한다.

'_' 기호는 앞선 모든 기호에 적용될 수 있으며,

Table 2. Attributes of stage node

| sym. | attribute | description |
|---|---|---|
| ∧ | AND | essential condition |
| ∨ | OR | optional condition |
| 〉 | Extra | extra condition |
| _ | simultaneous | simultaneous condition |

연결된 노드가 동시에 수행될 수 있는 경우를 의미한다. 해당 기호가 없는 경우에는 노드의 순서 번호에 따라 순차적으로 공격이 진행된다.

#### 3.2.3 S-CAFG 예시

Fig. 6은 훈련자의 행위에 따라 공격 기법 및 우회 경로를 가지는 Flooding 공격 시나리오를 S-CAFG로 표현한 것이다. S-CAFG의 Stage 1 노드는 네트워크 스캐닝 공격 단계에서 사용될 수 있는 공격을 정의하는 세 개의 하위 노드를 가진다. 이때, 시나리오의 공격 순서는 노드에 명시된 번호대로 실행된다.

시나리오의 흐름이 네트워크 스캐닝 공격 성공을 의미하는 stage 1 노드에 도달하기 위해서는 노드 아래에 위치한 조건식을 만족해야 한다. 노드 1.1과 1.2의 실행 결과는 반드시 성공해야 하며, '_' 기호를 가지므로 동시에 실행될 수 있다. 노드 1.3은 해커가 더 다양한 정보를 얻기 위해 수행하는 부가적인 공격이므로 수행되지 않거나 실패해도 stage 도달에 영향을 미치지 않는다.

Stage 2는 Flooding 공격 목표에 도달할 수 있는 2가지 경로를 가진다. 첫 번째로 실행되는 경로는 syn flooding 공격이다. 노드 2.1이 공격에 성공할 경우 공격 성공 노드인 stage 2에 즉시 도달할 수 있다. 하지만 네트워크 스캐닝 단계에서 IP 차단으로 인해 노드 2.1이 실패한 경우, IP를 변경하는 2.2 노드로 분기하여 Land 공격을 시도한다.

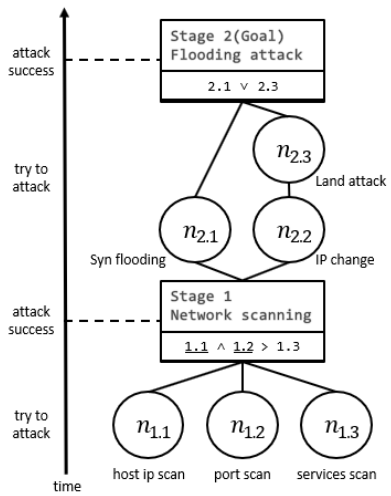



Fig. 6. Modeling a flooding attack using S-CAFG

이처럼 S-CAFG 모델은 복잡한 시나리오의 흐름을 효과적으로 모델링할 수 있다. 특히 특정 공격에 실패했을 경우, 다시 하위 노드로 돌아가 조건을 만족하는 다른 노드로 향하는 우회 공격 표현이 가능하다. 또한 공통 경로를 가지는 노드를 통합하고 트리 구조의 상향식 공격 흐름을 유지하여 보다 간결하게 공격 시나리오를 표현한다. 또한 공격 단계를 stage 노드로 구분하여 채점 및 훈련 평가 기준을 보다 명확히 할 수 있다.

## IV. 평 가

본 장에서는 S-CAFG를 평가하기 위해 가상의 공격자가 가상화폐 채굴 스크립트를 주입하는 사이버 공격 훈련 시나리오를 개발한 뒤 개선된 트리 모델인 D-CAT와 본 논문이 제안하는 S-CAFG로 모델링하였다. 이 시나리오는 동시 공격, 부가적인 공격, 우회 경로 선택과 더불어 기다림 상태 등 복잡한 네트워크 공격을 모사하기 때문에 기존의 모델링 기법으로는 표현하기 까다롭게 제작했다. 다만, 이 시나리오가 기존에 보고되지 않은 새로운 공격 기법이나 침투 경로를 가지는 것은 아니므로 S-CAFG와 기존의 트리 모델의 시나리오 표현 능력을 공정히 비교할 수 있다.

### 4.1 평가 시나리오

개발한 시나리오는 가상화폐 채굴 스크립트가 서비스 중인 웹 서버에 침투하는 공격을 모사했다. 채굴 스크립트는 XSS(Cross-site scripting) 공격 또는 파일 업로드 취약점을 악용한 command execution 공격을 통해 서버에 삽입된다. 삽입된 채굴 스크립트는 사용자가 오염된 웹 페이지를 이용할 때 자동으로 동작하며, 사용자의 컴퓨터 자원을 무단으로 사용하여 가상화폐를 채굴하고 공격자에게 전송한다.

시나리오의 상세한 정의는 Table 3과 같다. Attack 1은 네트워크 정보 수집은 공격 대상의 열린 포트와 서비스를 식별한다. 각 노드의 실행 결과가 다음 단계(노드)로 넘어가기 위한 조건을 만족하면 go to가 지정하는 단계로 이동한다. Attack 2.1은 XSS 공격을 통해 채굴 악성코드를 주입하는 공격을 수행한다. 공격은 노드의 번호순으로 진행하

Table 3. Cryptocurrency mining script injection scenario.

1. Cryptocurrency mining script injection
- Goal : Mining script injection
- Pre-condition : No mining script blocking rules in firewall
- Condition : '∧'(AND), '∨'(OR), '〉'(Extra), '_'(Simultaneous)
- go to : conditional jump

2. Attack
- Attack 1: Gathering service information
  - node 1.1 : Port scanning
  - node 1.2 : Open services scanning
  - node 1.3 : OS information scanning
  - node 1.4 : Vulnerability scanning
  condition 1 : 1.1 ∧ 1.2 〉 1.3 〉 1.4
  condition 2 : 1.1 ∧ 1.2 ∧ 1.3 〉 1.4
  go to 1 : Attack 2
  go to 2 : Attack 3

- Attack 2.1 : Mining script injection
  - node 2.1 : XSS
    - node 2.1.1 : Stored XSS
    - node 2.1.2 : Reflected XSS
    - node 2.1.3 : DOM-based XSS
  condition : 2.1.1 ∨ 2.1.2 ∨ 2.1.3
  go to : node 4

- Attack 2.2 : Command execution
  - node 2.2 : File upload (webshell)
    - node 2.2.1 : Fake extension file
    - node 2.2.2 : Obfuscation file
  condition : 2.2.1 ∨ 2.2.2
  go to : node 3

- Attack 3 : Mining script install
  - node 3 : Mining script install
  condition : must 3
  go to : node 4

- Attack 4 : Cryptocurrency mining (goal)
  - node 4 : Wait victim access

며, 각 노드는 서로 다른 유형의 XSS 공격을 의미한다. Attack 2.1의 모든 하위 노드는 OR로 연결되어 있으므로 한 가지 이상 XSS 공격이 성공하면 희생자를 기다리는 node 4로 이동한다.

Attack 2.2는 Attack 2.1에서 모든 XSS 공격(node 2.1.1~2.1.3)이 실패했을 경우 수행된다. 이 공격 단계는 Attack 1에서 획득한 운영체제 정보를 바탕으로 공격에 적합한 웹쉘을 파일 업로드 취약점을 통해 업로드한다. 파일 업로드 공격 유형은 node 2.2.1과 2.2.2로 두 가지 유형이 있으며, OR로 연결되어 있으므로 하나의 공격이 성공하면 악성 스크립트를 다운로드하는 node 3을 거쳐 node 4로 이동한다. 다만, stage 2.2는 Attack 1에 정의된 condition 2를 만족해야 하므로 이 조건을 만족하지 못한다면 최종적으로 해커의 공격은 실패한다.

## 4.2 D-CAT 기반 모델링

Fig. 7은 위 시나리오를 트리 기반 모델링 기법인 D-CAT으로 표현한 것이다. 이 모델은 각 공격 단계별 목표 노드에 대한 흐름은 효과적으로 표현할 수 있지만 Table 3과 같은 복잡한 시나리오를 완벽하게 표현할 수는 없었다. 예를 들어, $n_{12}$노드에 도달하기 위한 하위 노드 중 $n_{16}$은 해커가 추가적인 정보를 얻기 위해 수행하는 부가적인 공격으로 확률적으로 수행된다. 또한 상위 노드로 향하기 위한 조

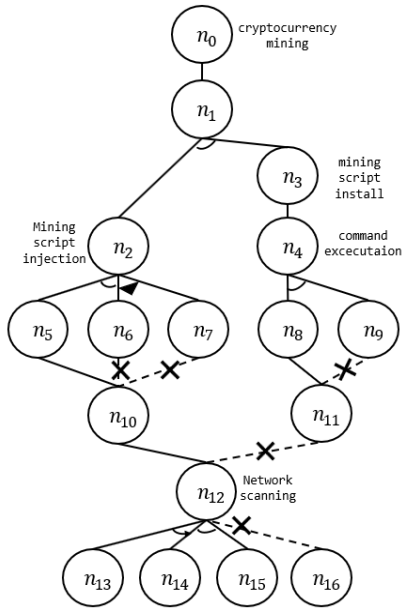



Fig. 7. Cryptocurrency mining script injection scenario modeling using D-CAT(X label is an impossible expression)

건에 영향을 미치지 않는다. D-CAT 모델은 이러한 $n_{16}$의 특성을 명확히 표현할 수 있는 기호가 없었다.

또한 노드 $n_{10}$, $n_{11}$, $n_{12}$은 모두 여러 갈래의 조건부 공격 흐름을 가진다. $n_{10}$의 경우에는 상위 노드인 $n_5 \sim n_7$을 순차적으로 실행하여 하나 이상의 공격이 성공하면 상위 노드로 이동한다. 이 시나리오는 만약 $n_5$가 실패하면 변형된 공격인 $n_6$을 수행하므로 이는 상향식 표현 방식에 어긋난다. 또한 트리 구조에서 자식 노드는 두 개 이상의 부모 노드를 가질 수 없다. 따라서 Table 3 시나리오와 같이 복잡한 조건부 분기를 가지는 시나리오는 기존의 모델로 표현하기 어려운 것을 확인할 수 있다.

### 4.3 S-CAFG 기반 모델링

Fig. 8은 table 3의 시나리오를 S-CAFG로 표현한 것이다. Stage 1은 해당 stage를 만족시키기 위한 하위 노드들의 조건을 명시한다. 이때 stage 1

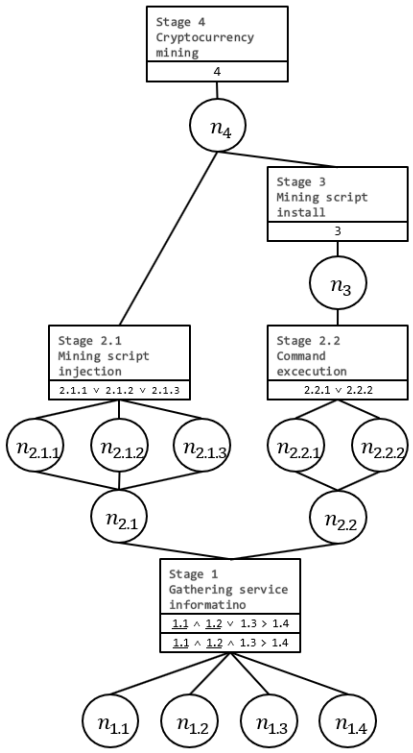



Fig. 8. Cryptocurrency mining script injection scenario modeling using S-CAFG

은 두 가지 공격 유형으로 분기하므로 각 분기에 해당하는 조건을 모두 명시한다. 예를 들어, 첫 번째 조건식이 만족하면 $n_{2.1}$로 분기하며 두 번째 조건이 만족하는 경우 $n_{2.2}$로 분기한다. 두 조건이 모두 만족하면 순서가 더 빠른 $n_{2.1}$이 우선 실행된다. 또한 각 조건식은 동시 실행과 부가적인 공격을 모두 명시하므로 복잡한 공격 시나리오를 효과적으로 표현할 수 있다.

노드 $n_{2.1}$과 $n_{2.2}$은 더 상세한 공격 유형으로 분기하여 같은 유형의 공격이라도 다양한 방법으로 수행되는 모습을 보여준다. 여기서 $n_{2.1.1}$과 같은 노드는 하위 노드인 $n_{2.1}$의 변형 공격을 의미한다. 또한 $n_3$은 희생자의 행위를 기다리는 상태를 표현한다. 이처럼 S-CAFG는 기존 모델이 표현할 수 없었던 복잡한 우회 경로 및 공격의 조건 분기를 모두 효과적으로 표현하는 것을 확인할 수 있다.

## V. 결 론

본 논문은 현대의 복잡한 사이버 공격을 모사하는 사이버 공격 훈련 시나리오를 효과적으로 표현하기 위한 모델인 S-CAFG를 제안했다. S-CAFG는 기존 그래프 및 트리 모델이 가진 한계점을 극복하기 위해 두 모델의 장점을 결합하였다. 또한 공격 흐름 및 공격 유형 변경과 같은 복잡한 시나리오를 표현하기 위해 stage 노드를 도입했다. Stage 노드는 해커의 단계별 공격 목표 달성을 위한 조건을 명시하고 공격 과정에서 발생하는 다양한 공격 흐름을 효과적으로 표현한다.

또한 본 논문은 S-CAFG를 평가하기 위해 실제 사이버 공격 훈련 시나리오를 제작하고 기존의 모델링 기법과 비교했다. 이 시나리오는 동시 공격, 부가적인 공격, 우회 경로 선택, 기다림 상태 등 기존 모델링 기법으로는 표현하기 어려웠던 복잡한 행위들을 모사한다. 이 시나리오를 S-CAFG를 통해 모델링한 결과, 기존 트리 기반 모델링 기법으로 표현할 수 없는 다양한 시나리오 흐름을 효과적으로 표현할 수 있음을 확인했다. 따라서 S-CAFG를 통해 최신 사이버 공격 훈련 시나리오를 모델링하면 보다 효과적인 시나리오 표현 및 공격 단계별 채점 기준을 마련할 수 있을 것으로 판단된다.

향후 연구로는 Table 3과 같은 시나리오 정의 언

어를 바탕으로 S-CAFG를 자동으로 생성하는 도구를 개발할 예정이다. 또한 S-CAFG 기반 사이버 훈련 시나리오의 네트워크 환경 및 공격을 자동으로 구현하는 프레임워크를 구현하고 예측하지 못한 공격에 대한 시스템의 영향을 표현할 수 있는 모델에 대한 연구를 병행할 예정이다.

## References


[1] KISA, "Cyber Security Isuue Report 2020 Q3," https://krcert.or.kr/main.do

[2] Su-youn Hong, Kwang-soo Kim and Tae-kyu Kim, "The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training," Journal of the KIMST, 22(6), pp. 797-805, Dec. 2019.

[3] Cyberbit Range, https://www.cyberbit.com/

[4] AIT Cyber Range, https://cyberrange.at/

[5] Dong-hwa Kim, Yong-hyun Kim, Myung-Kil Ahn and Hee-jo Lee, "Automated Cyber Threat Emulation Based on ATT&CK for Cyber Security Training," Journal of The Korea Society of Computer and Information, 25(9), pp. 71-80, Sep. 2020.

[6] R. Nakata, and A. Otsuka, "CyExec*: Automatic Generation of Randomized Cyber Range Scenarios," In Proceedings of the 7th International Conference on Information Systems Security and Privacy, pp. 226-236, Feb. 2021.

[7] V. Saini, Q. Duan and V. Paruchuri, "Threat modeling using attack trees," Journal of Computing Sciences in Colleges, Vol. 23, pp. 124-131, Apr. 2008.

[8] B. Schneier, "Attack Trees," Dobb's Journal of Software Tools 24, pp. 21-29, Dec. 1999.

[9] Jung-ho Eom, Seon-ho Park, Tai M. Chung, "A Study on an Extended Cyber Attack Tree for an Analysis of Network Vulnerabilit," Journal of the Korea Society of Digital Industry and Information Management, 6(3), pp. 49-57, Sep. 2010.

[10] Jung-ho Eom, "An Architecture of a Dynamic Cyber Attack Tree: Attributes Approach," Journal of the Korea Institute of Information Security & Cryptology, 23(3), pp. 67-74, Jun. 2011.

[11] Jung-Kuk Seo et al., "Adapted Attack Tree for Internet Attack Simulation," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 1200-1203, Nov. 2011.

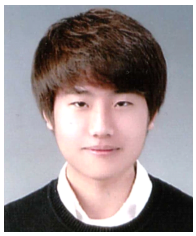
[12] Jung-Kuk Seo et al., "Attack Modeling for an Internet Security Simulation," The KIPS Transactions(partC), pp. 183-192, Apr. 2004.

[13] Joo-young Lee, Dae-sung Moon and Ik-kyun Kim, "Technological Trends in Cyber Attack Simulations," Electronics and Telecommunications Trends, 35(1), pp. 34-48, Jan. 2020.

[14] S. Jajodia, S. Noel, and B. O'berry, "Topological analysis of network attack vulnerability," Managing Cyber Threats, pp. 247-266, Jan. 2005.

[15] I. Kotenki and M. Stepashkin, "Attack graph based evaluation of network security," IFIP International Conference on Communications and Multimedia Security, pp. 216-227, Oct. 2006.

## 〈저자소개〉



김 문 선 (Moon-Sun Kim) 학생회원
2020년 2월: 한남대학교 컴퓨터통신무인기술학과 졸업
2020년 3월~현재 : 한남대학교 컴퓨터공학과 석사과정
〈관심분야〉 시스템 보안, 네트워크 보안, 바이너리 분석

이 만 희 (Man-Hee Lee) 종신회원
1995년 2월 경북대학교 컴퓨터공학과 공학사
1997년 2월 경북대학교 공학석사
2008년 8월 Texas A&M 대학교 컴퓨터공학과 공학박사
1997년~2003년 한국과학기술정보연구원 연구원
2008년~2009년 Cisco Systems, San Jose
2010년~2012년 국가보안기술연구소 선임연구원
2012년~현재 한남대학교 부교수
〈관심분야〉 네트워크/시스템/스마트폰 보안, 고성능 시스템, 컴퓨터교육