J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

사이버공격에 의한 임무피해 평가를 위한 모델 구현에 관한 연구☆

A Study on the Implementation of a Model for Mission Impact Assessment due to Cyber Attacks

김 용 현[1*] 김 동 화[1] 이 동 환[1] 김 주 엽[1] 권 미 영[1] 안 명 길[1]
Yonghyun Kim Donghwa Kim Donghwan Lee Juyoub Kim Miyoung Kwon Myung Kil Ahn

요 약

물리적 자산에 가해진 사이버공격은 해당 자산이 수행하는 임무에 영향을 미친다. 다양한 사이버공격에 대해 자산의 자원이 어떤 영향을 받게 되고, 자산의 영향으로 인해 임무 수행에 피해가 어느 정도인가를 판단하기 위해 M&S(Modeling & Simulation) 기술을 활용할 수 있다. 사이버전에 의한 임무영향 분석 관련 연구는 미국을 중심으로 많이 수행되었다. 기존 연구는 사이버공격이 중요한 임무에 어떤 방식으로, 어느 정도까지 영향을 미치는지를 포착하기 위한 프레임워크와 방법론을 제공하지만, 임무환경과 사이버환경을 표현하는 모델 구축방법과 모델간의 연관관계가 구체적이지 못하다. 이러한 한계를 극복하기 위해 사이버공격과 임무 모델의 모의논리와 모델링에 대한 개발이 필요하다. 또한 자산에서 임무체계까지를 계층별로 분류하고, 계층간 연결관계를 정의한 후 계층간 피해가 전파되는 모델을 개발해야 한다. 본 논문에서는 계층간 종속관계를 이용하여 사이버공격에 의한 임무체계의 피해를 평가할 수 있는 모델의 모의방법과 M&S 기술을 활용하여 사이버전에 의한 임무 피해평가를 위한 모델을 구현하는 방법을 제안하고, 제안한 방법에 따라 구현한 모델을 제시한다. 본 논문에서 제안한 모델은 시범적으로 3종류의 임무체계를 대상으로 검증하였으며, 향후 군의 다양한 임무체계를 대상으로 사이버공격에 의한 임무피해평가를 정량적으로 분석할 것으로 기대된다.

☞ 주제어 : 사이버공격, 사이버 M&S, 임무피해 평가, 임무영향 분석, CyMIA

ABSTRACT

Cyber Attacks on physical asset impacts the missions the asset performs. To determine how the resources of an asset are affected by various cyber attacks and to assess the impact on mission performance due to the asset's condition, modeling & simulation technology can be utilized. Many studies on mission impact analysis due to cyber warfare have been conducted, primarily in the United States. Existing research provides frameworks and methodologies to capture how and to what extent cyber attacks impact critical missions. However, it lacks specificity in the construction of models representing the mission and cyber environment, as well as in the relationships between these models. To overcome these limitations, it is necessary to develop simulation logic and modeling for cyber attacks and mission models. In addition, it is necessary to classify from assets to mission systems by hierarchy, define the connections between the hierarchies, and develop the propagation of damage across these hierarchies. This paper proposes a simulation method for a model that can evaluate mission system damage caused by cyber attacks using inter-hierarchical dependencies, and presents a method for implementing a model for mission impact assessment due to cyber warfare. The model implemented according to the proposed method is also presented. The model proposed in this paper was tested on three types of mission systems as a pilot study. It is expected to quantitatively analyze mission damage assessments due to cyber attacks on various military mission systems in the future.

☞ keyword : Cyber Attack, Cyber M&S, Mission Damage Assessment, Mission Impact Analysis, CyMIA

1. 서 론

21세기 들어 정보통신 기술의 발달과 함께 사이버 공간이 새로운 전장으로 부상하였다. 사이버전은 전통적인 군사작전과는 달리 인터넷과 네트워크를 통해 적의 정보시스템을 공격하거나 방어하는 행위로 정의된다. 이는 국가 간의 군사적 충돌뿐만 아니라 테러리스트, 해커 그룹 등 다양한 주체에 의해 실행될 수 있으며, 그 영향 범위와 파괴력은 점차 확대되고 있다.

1 Cyber Technology Center, Agency for Defense Development, Seoul, 05771, Rep. of Korea.
* Corresponding author (yonghyunkim@add.or.kr)
[Received 10 July 2024, Reviewed 16 July 2024(R2 05 August 2024), Accepted 09 August 2024]
☆ 본 연구는 국방과학연구소 과제(912921301)의 지원을 받아 수행한 논문임

사이버전의 가장 큰 특징은 물리적 공간에서 이루어지지 않는 비대면 공격이라는 점이다. 이는 공격자의 위치를 파악하기 어렵게 만들고, 짧은 시간 내에 대규모 피해를 입힐 수 있는 잠재력을 지니고 있다. 특히, 국가의 핵심 인프라와 군사 시스템이 디지털화됨에 따라 사이버 공격의 위협은 더욱 현실적이고 중대해졌다. 사이버전은 단순히 데이터 탈취를 넘어, 전력망, 통신망, 금융 시스템 등 국가의 중요한 기반 시설에 직접적인 영향을 미칠 수 있으며, 이는 곧 국가 안보와 직결되는 문제로 대두되고 있다 [1].

사이버전에 의한 임무영향 분석은 이러한 사이버공격이 군사적 임무 수행에 어떤 영향을 미치는지를 평가하는 중요한 과정이다. 이는 사이버공격으로 인해 발생할 수 있는 다양한 형태의 손실과 그로 인한 작전 수행 능력 저하를 정량적으로 분석하고, 이를 바탕으로 대응책을 마련하는 데 필수적인 정보를 제공한다. 사이버전에 의한 임무영향 분석은 사이버공격의 잠재적 위협을 사전에 예측하고, 이에 대한 방어 전략을 수립하는데 중요한 역할을 한다 [1].

물리적 자산에 가해진 사이버공격은 해당 자산이 수행하는 임무에 영향을 미친다. 다양한 사이버공격에 대해 자산의 자원이 어떤 영향을 받게 되고, 자산의 영향으로 인해 임무 수행에 피해가 어느 정도인가를 판단하기 위해 M&S(Modeling & Simulation) 기술을 활용할 수 있다. M&S 기술을 이용하여 사이버전에 의한 임무 피해를 정량적으로 산출하기 위해서는 피해평가 모의방법과 모의 내용이 반영된 모델을 개발해야 한다 [2]. 사이버공격에 의한 임무체계의 피해를 분석하기 위해서는 자산에서 임무체계까지를 계층별로 분류하고, 계층간 연결관계를 정의한 후 계층간 피해가 전파되는 것을 개발해야 한다.

임무체계는 체계가 구동되는 자산, 자산에서 구동되는 서비스, 임무를 구성하는 과업으로 구분할 수 있다. 이를 계층화하고 계층간 종속관계를 수치화함으로써 사이버공격에 의한 임무피해평가를 수행할 수 있다. 본 논문에서는 계층간 종속관계를 이용하여 사이버공격에 의한 임무체계의 피해를 평가할 수 있는 모델의 모의방법과 M&S 기술을 활용하여 사이버전에 의한 임무 피해평가를 위한 모델을 구현하는 방법을 제안한다. 또한 제안한 방법에 따라 구현한 모델을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 사이버공격에 의한 임무영향을 분석하는 기존의 관련연구 내용을 소개한다. 3장에서는 임무 피해평가를 위한 모델의 구현 방법을 제안하고, 4장에서는 제안된 방법에 의해 구현한 모델을 제시한다. 5장에서 연구 결과를 요약하고, 결론 및 향후 연구방향에 대해 서술한다.

2. 관련연구

임무체계 운영에 사이버 인프라 의존도가 증가함에 따라 사이버공격에 의한 임무영향평가의 필요성이 커졌다. Jakobson [3]은 사이버 공격이 임무 결과에 미치는 영향을 모델링하고 분석하기 위해 IDGs(Impact Dependency Graphs)를 사용하는 새로운 접근 방식을 소개한다. Sun 등 [4]은 특정 사이버 공격에 대한 대응을 용이하게 하기 위해 IDG와 공격 그래프를 연결하는 새로운 그래픽 모델을 제안했다. Schneider 등 [5]는 사이버공격에 의한 영향을 측정하기 위해 공격 트리 접근 방식을 사용한다. Jajodia 등 [6]은 원시 보안 데이터를 공격 그래프로 변환하여 전체 네트워크 보안에 개별 및 복합 취약점이 어떻게 영향을 미치는지에 대한 공통 작업 이미지와 구체적인 이해를 제공한다.

Musman 등 [7]은 사이버 영향 평가를 처리하기 위한 대안적인 접근법을 제안했다. 복잡한 임무에 대한 사이버 공격의 영향을 계산하는 CMIA(Cyber Mission Impact Assessment) 프레임워크는 임무 목표를 달성하는데 중요한 것이 무엇인지 이해함으로써 임무 영향을 평가하려고 한다. Cyber-ARGUS [8]는 영향 평가를 위해 일반적인 임무 관점 접근법을 따른다. Musman 등과 Jajodia 등과는 달리, 제안된 방법론은 임무와 인프라 개념을 매핑하는 방법을 보여주며, 실제 시나리오에서 사용할 수 있는 실용적 모델을 제공한다. Kaixing 등 [9]은 CPS (Cyber-Physical Systems) 환경에서 사이버 공격이 발생했을 때 실제 시설에 얼마만큼의 물리적 피해가 가해졌는지에 대한 연구를 수행하였으며, 베이지안 네트워크를 통해 공격 전파 과정을 추론하여 센서 및 장비의 손상 정도와 확률을 계산한다.

미국의 MITRE에서는 사이버 공격 및 방어에 의한 임무의 영향 분석을 위해, AMICA(Analyzing Mission Impacts of Cyber Action) [10] 프로토타입을 공개했다. 이는 사이버 공격 및 방어 TTPs(Tools, Techniques, and Procedures)와 사이버 행동 방안 계획을 지원하는 다양한 시각화 도구와 통합된 시뮬레이션 모델을 포함한다. MITRE는 프로세스 모델링 도구를 이용하여 임무체계를 시뮬레이션 하고 사이버 공격의 임무 영향을 동적으로 계산할 수 있는 방법을 제시하였지만 프로세스 모델링을

위한 기존 COTS(Commercial Off the Shelf) 도구의 한계로 인해 연구 결과의 실제 적용이 방해를 받았다. 이러한 한계를 해결하기 위해 MITRE는 자체적인 사이버 임무 영향 비즈니스 프로세스 모델링 도구를 개발하였다 [11]. 이 도구는 비록 비즈니스 프로세스 모델링 표기법(Business Process Modeling Notation, BPMN)의 기능적인 하위 집합만을 구현했지만 보다 일반적인 COTS 도구와는 달리 사이버 프로세스, 자원 및 사이버 공격 효과를 표현하기 위해 특별히 설계되었다.

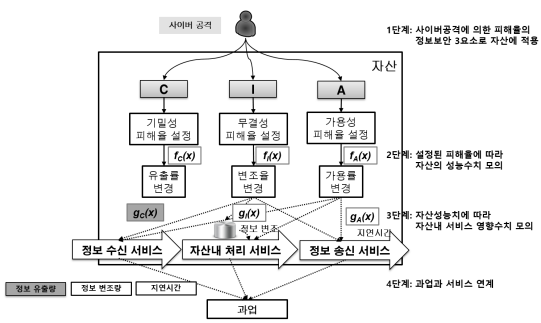
기존 연구는 사이버공격이 중요한 임무에 어떤 방식으로, 어느 정도까지 영향을 미치는지를 포착하기 위한 프레임워크와 방법론을 제공하지만, 임무환경과 사이버 환경을 표현하는 모델 구축방법과 모델간의 연관관계가 구체적이지 못하다. 이러한 한계를 극복하기 위해 사이버공격과 임무 모델의 모의논리와 모델링에 대한 개발이 필요하다.

3. 임무 피해평가를 위한 모델 구현 방법

본 장에서는 사이버공격에 의한 임무체계 피해산출을 위한 모델을 구현하기 위한 모의방법과 모델을 구현하는 방법에 대해 기술한다.

3.1 피해산출을 위한 모델의 모의 방법

임무체계는 자산, 서비스, 과업, 임무로 계층화하여 표현할 수 있다. 임무체계를 수행하는 자산은 네트워크를 통해 연결되며 가장 하위 계층에 배치된다. 자산은 서비스를 활용하여 과업을 절차에 맞춰 수행하고, 과업이 성공적으로 수행되면 임무는 완료된다. 이때 자산에 문제가 발생하게 되면 서비스가 영향을 받게 되고, 과업, 임무까지 영향을 받게 된다. 공격자는 자산의 취약점을 활용하여 공격을 수행하며, 자산은 기밀성, 무결성, 가용성 측면에서 피해가 발생하게 된다. 이로 인해 자산에서 구동되는 서비스는 정상적으로 동작이 안되며, 서비스를 활용하는 과업에도 영향을 미친다. 최종단인 임무는 과업의 피해로 인해 임무가 지연되거나 실패할 수도 있게 된다.



(그림 1) 자산의 피해반영 절차
(Figure 1) Asset Damage Reflection Procedure

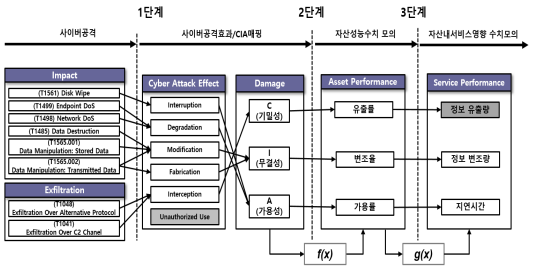
사이버공격은 자산으로부터 시작이 되는데 사이버공격에 의해 자산이 피해를 받는 것을 모의하는 것이 중요하다. 그림 1은 자산이 사이버공격을 받았을 때 자산이 받게 되는 피해를 단계별로 절차화한 것이다.

3.1.1 사이버공격과 사이버공격효과/CIA 매핑 모의

피해반영의 첫 번째 단계는 공격자가 수행한 사이버공격의 피해를 자산에 적용하기 위해서 자산의 피해분석 대상을 기밀성(C), 무결성(I), 가용성(A)으로 구분하고, 사이버공격을 C/I/A로 매핑한다. 이를 위해 사이버공격과 사이버공격효과를 먼저 매핑한 후, 사이버공격효과와 C/I/A를 매핑한다.

그림 2는 사이버공격을 사이버공격효과와 CIA로 매핑한 것을 나타낸 것이다. 사이버공격의 목표는 MITRE의 ATT&CK Impact 내용을 참조해서 사이버공격효과와 매핑하였다. 사이버공격효과는 다양한 연구가 있지만 표준화된 내용이 없어서 MITRE의 Musman이 제안한 내용 [7]과 이를 최종 5가지로 분류한 Melanie Bernier 연구결과 [12]를 활용하였다. 5가지 사이버공격효과는 공격에 의해 정보 자산을 사용하지 못하게 되거나, 일정 시간 자산을 사용 불가 상태로 만드는 공격 행위인 Interruption, 자산의 수행 능력을 하락시키는 공격 행위인 Degradation, 자산의 정보, 데이터, 프로토콜 등을 수정하는 공격 행위인 Modification, 공격자의 특정 데이터를 자산에 삽입시키는 공격 행위인 Fabrication, 정보를 중간에 탈취하거나 정보가 새도록 하는 공격 행위인 Interception이다.

사이버공격효과와 정보보안 3요소인 기밀성(C), 무결성(I), 가용성(A)의 매핑도 Melanie Bernier 연구결과를 활용하였다. 사이버공격-사이버공격효과-CIA 매핑을 통해 공격자가 수행하는 공격의 종류와 그로 인해 자산이 받게 되는 피해율이 연결된다. 즉, 시뮬레이션을 위한 시나리오에서 공격자가 사이버자산에 가하고자 한 피해율을 설정하게 되면, 자산의 정보자산 3요소의 해당내용의 피해율에 반영되게 된다.



(그림 2) 사이버공격, 사이버공격효과, CIA 매핑
(Figure 2) Cyber Attack, Cyber Attack Effect, CIA Mapping

3.1.2 자산성능 수치 모의

피해반영의 두 번째 단계는 사이버공격의 피해율을 자산의 성능수치로 반영하는 것으로 설정된 피해율에 따른 자산의 유출률, 변조율, 가용률을 정량적으로 모의해야 한다. 공격자가 의도한 피해율은 다양하게 표현할 수 있지만, 피해율이 높으면 성능수치도 비례해서 높게 표현하는 것이 가장 일반적이다. 따라서 공격자가 의도한 피해율에 대한 자산의 유출률과 변조율은 선형적으로 모의하였다. 공격자가 의도한 피해율에 대한 자산의 가용률은 컴퓨터 시스템에서 일반적으로 통용되는 자료 [13]를 참조하여 식 (1)과 같이 모의하였다.

$$f_A(x) = \frac{1}{1 + e^{-k(x - x_0)}} \tag{1}$$

여기서 x는 공격자가 의도한 가용성의 피해율을 나타내며, k는 가용률에 대한 기울기를 결정하는 상수이다. x_0는 오프셋이며 $0 \le x_0 \le 1$ 범위를 갖는다. 공격자가 의도한 가용성의 피해율 x는 다양한 요소로 구성 가능하며, 식 (2)는 CPU와 메모리로 구성한 것이다.

$$x = \lambda_{cpu}(1 - x_{cpu}) + \lambda_{mem}(1 - x_{mem}) \tag{2}$$

여기서 공격자가 CPU에 가해지는 피해율의 범위는 $0 \le x_{cpu} \le 1$이며, 공격자가 메모리에 가해지는 피해율의 범위는 $0 \le x_{mem} \le 1$이다. 가용률은 공격자가 가하는 피해율이 어느 변곡점 주변에서 가파르게 변화하는 로지스틱 곡선 형태를 나타내고, 피해율이 최대치이면 가용률이 0이 되어야 한다. 이를 충족시키기 위해 공격자가 가하는 피해율은 최대값 1에서 빼주는 형태를 사용하였다. λ는 CPU, 메모리에 대한 가중치를 나타내며, CPU와 메모리의 가중치의 합은 식 (3)과 같다.

$$\lambda_{cpu} + \lambda_{mem} = 1 \tag{3}$$

3.1.3 자산내 서비스 영향 수치 모의

피해반영의 세 번째 단계는 자산의 성능치에 따라 자산내 서비스가 받게되는 영향을 수치로 반영하는 것이다. 자산의 성능치는 유출률, 변조율, 가용률로 나타낸다. 자산내 서비스는 다른 자산과 정보를 주고 받는 송수신 기능과 자산내에서 처리하는 기능으로 분류할 수 있으며, 자산의 성능치에 따라 영향을 받게 된다. 정보 유출은 아군의 정보 탈취에 의한 적군의 행위가 변경되어야 하는 유형의 사이버공격인데, 적군의 행위는 시나리오에 사전 설정으로 모의함에 따라 유출률은 사이버 임무영향 평가에서 제외한다. 변조율은 정보 변조량을 산출하는 것으로 정보의 흐름에서 정보의 변조가 발생할 경우 아군의 행위가 최초 과업 생성 시 설정된 정보가 변조되어 시나리오가 전개됨에 따라 임무 효과도의 변화를 발생한다. 사이버공격의 대상은 자산이 보유한 정보이며 정보는 N개의 세부 정보를 포함한다. 세부 정보는 정량적인 수치를 가지는 값과 그 외의 데이터로 구분할 수 있다. 정량적 수치의 값의 경우 변조율에 의하여 수치를 변경하고, 그 외의 데이터 값은 원본 데이터가 아닌 그 외의 임의의 값으로써 해당 필드가 가질 수 있는 값의 범위 내에서 무작위로 추출한다. 가용률은 지연시간을 산출하는 것으로, 가용성 공격에 의하여 자산의 성능이 감소할 경우 감소된 비율 만큼 서비스 수행에 소요되는 시간은 증가한다. 가용률에 의한 지연시간 모의는 식 (4)를 이용한다.

$$g_A(x) = \frac{\text{현재처리량}}{\text{최대처리용량} \times x} \tag{4}$$

여기서 현재처리량은 현재 패킷 처리 요구량을, 최대처리용량은 초당 최대 패킷 처리 가능 용량은 나타낸다. x는 자산의 가용률이며, 범위는 $0 \le x \le 1$ 이다.

3.1.4 과업과 서비스 연계 모의

피해반영의 네 번째 단계는 자산의 서비스와 서비스를 활용하는 임무 과업을 연계시키는 것이다. 자산의 서

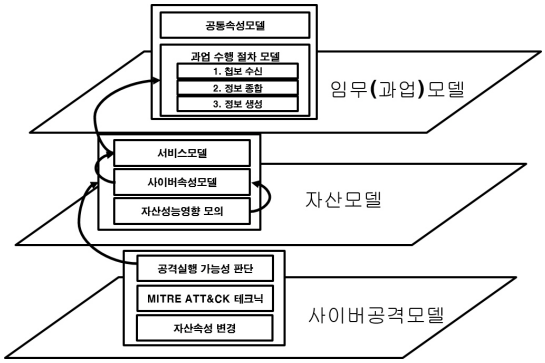
비스는 그림 1에서 알 수 있듯이 다른 자산으로부터 정보를 수신하는 서비스, 자산내에서 정보를 처리하는 서비스, 생산된 정보를 다른 자산으로 송신하는 서비스로 구분한다. 과업은 자산의 서비스를 통해 수행되는데 이런 관계를 모델링에 포함해 주어야 한다. 이를 위해서는 자산모델 속성에 서비스가 포함되어야 하고, 과업모델에는 자산의 서비스를 연결해 주는 절차를 포함하여 시나리오 저작과정에서 설정한다. 자산모델과 과업모델의 연결을 통해 사이버공격에 의한 과업의 영향은 자산의 서비스 피해영향 수치를 이용하여 정량적으로 산출할 수 있다.

3.2 임무 피해평가를 위한 모델 구현 방법

사이버공격에 의한 임무체계의 피해를 평가하기 위해서는 임무체계를 표현하는 모델, 구축된 모델을 이용하여 시뮬레이션을 준비하는 기능, 시뮬레이션 결과를 이용하여 분석하는 기능이 필요하다. 따라서 임무 피해평가 모델을 구현하기 위해서는 3가지 요소가 모두 포함되어야 하며, 이를 위해 3단계로 구분하여 구현한다. 첫 번째 단계는 모델 구축 단계로 임무 피해평가 모의 방법을 적용한 모델을 구현하고, 두 번째 단계는 시뮬레이션 준비단계로 임무시나리오 저작시 구현한 모델을 연계시키는 방법을 구현한다. 세 번째 단계는 시뮬레이션 이후 분석 단계로 시뮬레이션 결과로부터 임무피해를 정량적으로 산출하는 방법을 구현한다.

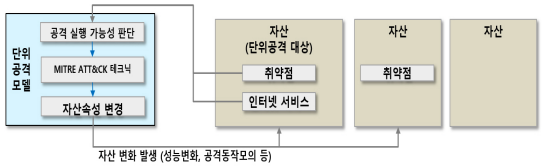
3.2.1 피해산출 모의 방법을 적용한 모델 구현방법

그림 3은 임무 피해평가를 위해 필요한 모델과 모델간 연계도를 나타낸 것이다. 자산에 사이버공격을 가하면 자산과 연계된 임무는 영향을 받게 된다. 이러한 과정은 모델로 구현되어야 하며, 구현된 모델에 사이버공격부터 그로 인한 피해평가를 산출할 수 있는 속성을 모델에 반영하여야 한다. 임무피해평가를 위해서는 사이버공격모델, 자산모델, 임무를 수행하는 과업모델이 필요하다. 사이버공격모델을 이용하여 자산모델을 공격하고, 자산모델 내에서는 사이버공격에 대한 자산성능영향 모의결과를 반영할 사이버속성모델과 서비스모델을 구현하여야 한다. 임무의 세부 절차인 과업모델은 과업 수행 절차 모델에서 자산모델 내 서비스모델을 이용하게 된다. 이렇게 모델간 연계를 모델내 속성에 반영함으로써 사이버공격에 의한 임무체계 피해평가를 수행할 수 있다.



(그림 3) 피해평가를 위한 모델 연계도
(Figure 3) Model Connectivity Diagram for Damage Assessment

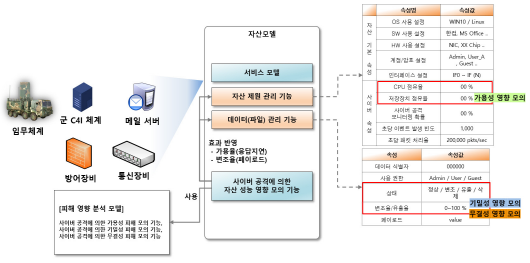
그림 4는 사이버공격을 위한 단위공격모델 구성 및 모델의 진행 순서도이다. 단위공격모델은 사이버공격을 위한 최소단위를 모델화한 것으로 공격 실행 가능성 판단 모듈, MITRE ATT&CK 테크닉 기반 공격 실행 모듈, 자산 속성 변경 모듈로 구성한다. 공격 실행 가능성 판단 모듈은 자산의 취약점이나 자산에서 실행중인 인터넷 서비스(웹, 메일, DB 등)에 기반한 공격 실행 가능성을 판단한다. 공격 실행이 가능하면, MITRE ATT&CK 테크닉 기반 공격 실행 모듈은 취약점이나 인터넷 서비스에 해당하는 MITRE ATT&CK 테크닉을 이용하여 공격을 수행한다. 사이버공격에 의해 자산은 피해를 받게 되는데 자산 속성 변경 모듈은 자산모델의 속성에 피해를 반영한다. 사이버공격은 단일 단위공격모델로 진행할 수 있으며, 여러 개의 단위공격모델을 연결해서 진행할 수 있다.



(그림 4) 사이버공격을 위한 단위공격 모델
(Figure 4) Unit Attack Model for Cyber Attacks

자산모델은 그림 5와 같이 자산 제원 관리 기능, 데이터(파일) 관리 기능, 사이버 공격에 의한 자산 성능 영향 모의 기능, 서비스 모델로 구성이 된다. 자산 제원 관리 기능은 자산 기본 속성과 사이버 속성으로 구분한다. 자산 기본 속성은 자산을 구성하는 하드웨어, 소프트웨어,

계정, 인터페이스 정보에 대한 내용을 관리한다. 사이버 속성은 사이버 공격 및 방어 모의와 관련된 내용을 속성으로 관리하는 것이다. 사이버공격에 의해서 자산의 제원의 변화(CPU 점유율, 저장장치 점유율, 데이터 변조 등)와 공격의 진행상태를 속성으로 관리한다. 또한 사이버 방어 자산의 설정상태와 변화를 관리하고, 사이버 공격에 대한 모니터링 확률 등도 관리한다. 데이터(파일) 관리 기능은 자원내에서 임무와 관련된 데이터나 파일, 사이버공격에 사용될 수 있는 데이터나 파일, 계정정보, 암호 정보를 관리한다. 사이버공격에 의한 자산 성능 영향 모의 기능은 3.1절에서 제안한 모의방법을 수행한다. 즉, 사이버공격의 피해를 정보보안 3요소인 기밀성, 무결성, 가용성으로 나눠서 자산의 속성에 반영한다. 그림 5에 자산성능 영향 모의 기능에 의해 자산 제원과 데이터(파일)의 속성에 기밀성, 무결성, 가용성 측면의 영향을 적용하는 예시를 나타냈다.



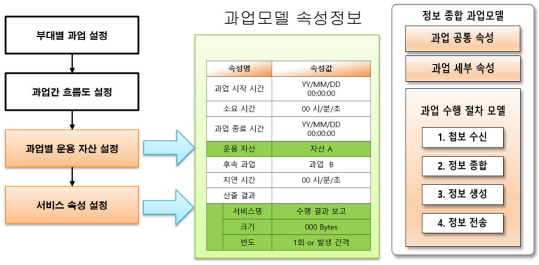
(그림 5) 자산모델 속성 및 자산성능 영향 모의 기능
(Figure 5) Asset Model Attributes and Asset Performance Impact Simulation Function

자산모델 내 임무(과업) 관련 서비스는 자산내 처리 서비스, 정보 송·수신 서비스가 있다. 자산내 처리 서비스는 자산에서 구동되는 응용체계의 기능으로써 하나의 과업을 수행하는데 사용한다. 정보 송·수신 서비스는 생산된 정보를 전송하거나, 정보를 수신하는 것으로, 과업과 과업을 연계시켜주며 서비스가 구동되는 자산은 상이할 수 있다. 3가지 서비스 모델은 과업모델의 과업 수행 절차 모델과 연계가 된다. 자산내 처리 서비스는 과업 수행 절차의 처리시간에 영향을 주는 요소로 본 논문에서는 과업 수행 절차의 처리시간에 서비스 지연시간을 반영하는 형태로 서비스를 대체한다. 정보 송·수신 서비스는 자산에서 생산된 정보를 전송하거나 수신하는 것으로, 본 논문에서는 통신특성을 설정하는 방식으로 모의한다. 송신자산, 수신자산, 패킷크기, 발생주기 등을 속성으로 해서 서비스 모델을 구현한다.

과업모델은 공통속성, 세부속성, 과업 수행 절차로 구성이 된다. 공통속성에는 과업마다 공통되는 속성을 관리하는 것이고, 세부속성은 과업의 소요시간을 관리한다. 과업 수행 절차는 각 과업의 내부 처리 절차를 모의해 놓은 것으로 자산모델의 서비스 모델과 연계시켜서 수행된다. 과업 수행 절차는 과업의 시작부터 과업의 종료까지가 순서에 따라 수행된다. 과업 시작은 설정된 지정시간에 시작하거나 선행과업이 지정이 되어 있으면 선행과업 종료 후 실행된다. 과업 수행 시간은 지연시간까지가 포함된 시간을 저장하게 되고, 차후 시뮬레이션 결과 분석 과정에서 활용하게 된다.

3.2.2 임무시나리오 저작시 구축된 모델 연계 방법

임무시나리오는 부대에 주어지는 임무를 과업모델을 이용하여 저작하는 것이다. 임무는 여러 개의 과업으로 나눌 수 있으며, 각각의 과업에 해당하는 과업모델을 선택한다. 과업은 선후 진행조건에 따라 서로 연결을 시키고, 과업모델의 속성을 설정한다. 과업모델 속성에는 자산모델과의 연결고리를 반영하여, 그림 6과 같이 과업모델 속성 설정 과정에서 이를 설정할 수 있게 한다. 과업별 운용 자산 설정과 서비스 속성 설정 과정이 이에 해당한다. 과업별 운용 자산 설정은 과업모델이 구동되는 자산모델을 설정하면 되고, 서비스 속성 설정은 자산모델에 기 구축되어 있는 서비스모델을 선택하거나 신규로 등록해서 연결해주면 된다.

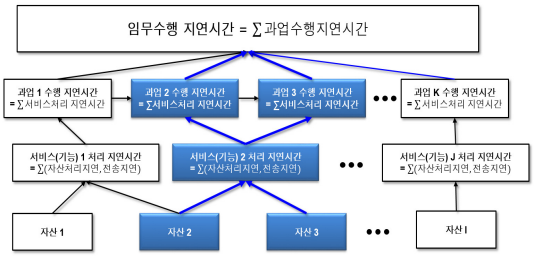


(그림 6) 과업모델 속성 설정
(Figure 6) Task Model Attribute Configuration

3.2.3 시뮬레이션 결과로부터 임무피해 산출 구현방법

그림 7은 시뮬레이션 결과로부터 임무피해를 정량적으로 산출하는 방법에 관한 것이다. 본 논문에서는 사이버공격에 의한 임무체계의 피해평가를 그림 3에서와 같

이 모델간 계층적 연결구조를 이용하여 분석하는 것으로 했다. 구현한 모델의 속성에 피해평가를 수행하는 모의 논리를 반영하였으며, 시나리오 저작시 모델의 속성에 모델간의 연결관계를 설정하였다. 시뮬레이션을 수행하면 모델간 연결관계에 의해 시뮬레이션 결과는 모델의 속성에 저장이 된다.



(그림 7) 시뮬레이션 결과로부터 임무피해 산출 절차
(Figure 7) Procedure for Deriving Mission Damage from Simulation Results

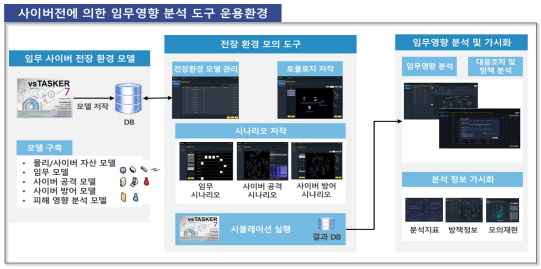
사이버공격으로 인해 임무에 영향을 미치는 요소는 자산의 가용성으로 인한 임무 수행 시간 지연과 자산의 정보변조나 탈취로 인한 적 피해율 변화, 임무의 착오율 변화 등이 있다. 영향을 미치는 요소 중 가장 중요한 것이 임무 수행 지연시간이다. 임무 수행 지연시간은 식 (5)와 같이 과업수행 지연시간의 총합이 되며, 과업수행 지연시간은 과업을 수행시 사용하는 서비스 처리 지연시간이 된다. 자산에서 구동되는 서비스모델은 자산내 처리 서비스나 정보 송·수신 서비스에서 각각 자산내 처리시간 지연과 전송시간 지연이 발생한다. 이러한 서비스모델의 지연시간을 합한 결과가 과업의 지연시간의 합에 이용되고, 최종 임무 수행시간의 합으로 산출된다. 정량화된 수치로 산출된 임무수행시간은 임무가 재시간에 수행되었는지를 판단할 수 있다.

$$\begin{aligned} \text{임무수행 지연시간} &= \sum_{i=1}^{K} \text{과업}\,i\,\text{수행 지연시간} \\ &= \sum_{i=1}^{J} \text{서비스}\,i\,\text{처리 지연시간} \\ &= \sum_{i=1}^{J} \text{자산}\,i(\text{자산처리 지연, 전송 지연}) \end{aligned} \quad (5)$$

4. 임무 피해평가를 위한 모델 구현 결과

본 장에서는 3장에서 설명한 사이버공격에 의한 임무 피해평가 모델 구축 방법에 따라 구현한 결과를 제시한다. 임무 피해평가 모델은 제안한 방법에 따라 상용 시뮬레이터 엔진(vsTASKER) 기반에서 C++으로 개발하였다. 임무 피해평가를 위한 모델은 속성과 모델의 모의논리와 모의에 의해 발생하는 속성값 변경을 위한 기능으로 구성된다. 속성값은 데이터베이스로 구현하여 관리하며, 기능은 C++로 코딩된 모델의 모의논리를 컴파일을 통해 시뮬레이터에서 동작한다.

구축된 모델은 웹서버 기반에서 구동되는 CyMIA 도구 [2, 14]를 통해 사용된다. 그림 8은 구축한 모델과 사이버전에 의한 임무영향 분석 도구 운용환경 및 구현 결과이다. CyMIA 운용환경은 시뮬레이션 엔진으로 vsTASKER 7.0과 DBMS엔진으로 MySQL로 구성된다. 전장환경 모의도구와 임무영향 분석 및 가시화는 Python과 JavaScript로 개발하여 웹기반으로 운용된다. CyMIA 운용서버는 Dell Precision 7920으로 Intel Xeon Silver 4214R 2.4G CPU와 16GB RAM을 탑재했다.



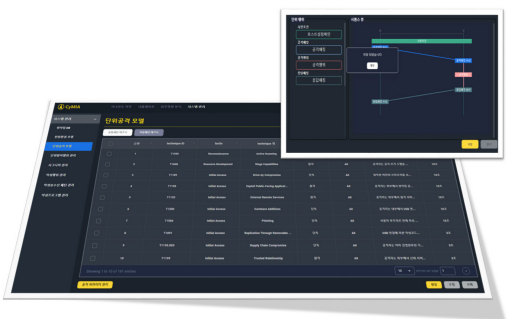
(그림 8) CyMIA 운용환경 및 구현 결과
(Figure 8) CyMIA Operating Environment and Implementation Results

4.1 임무 피해평가 방법을 적용한 모델 구현 결과

사이버공격에 의한 임무체계 피해평가를 위해 임무환경을 모의하는 자산 모델, 과업 모델을 그림 9와 같이 구축하였다. 임무를 수행하는 부대에서 운용하는 자산은 자산 모델을 이용하여 배치한다. 부대에서 수행하는 임무는 과업 모델을 이용하여 업무절차를 저작한다. 모델은 설계한 모의방법과 모의속성을 반영하였으며, 모델간 연계는 모델 속성에 반영하였으며, 시나리오 저작시 연계하도록 구현하였다.

(그림 9) 자산 모델, 과업 모델 구현 결과
(Figure 9) Implementation Results of Asset Model and Task Model

사이버공격 모델은 그림 10과 같이 MITRE의 ATT&CK 프레임크를 참조하여 단위공격 모델과 단위공격 모델간 연계모델을 구현하였다. CyMIA는 단위공격 모델을 구축하여 관리하며, 사이버공격 시나리오 저작시 가용할 단위공격 모델을 선택하고, 연계하여 적용한다.



(그림 10) 사이버공격 모델 구현 결과
(Figure 10) Implementation Results of the Cyber Attack Model

CyMIA 도구는 표 1에서와 같이 자산모델은 물리 자산 6종, 정보체계 자산 5종, 통신체계 자산 6종, 방어 자산 11종을 구현하였다. 과업모델은 감시정찰, 정보종합, 지휘결심, 화력지원, 화력운용 등 10종을 구현하였다. 사이버공격모델은 공통패턴 191종과 복합패턴 7종을 구현하였다.

4.2 모델간 연계 방법 구현 결과

사이버공격에 의한 피해평가를 산출하기 위해서는 구

(표 1) 모델 구현 결과
(Table 1) Implementation Results of the Model

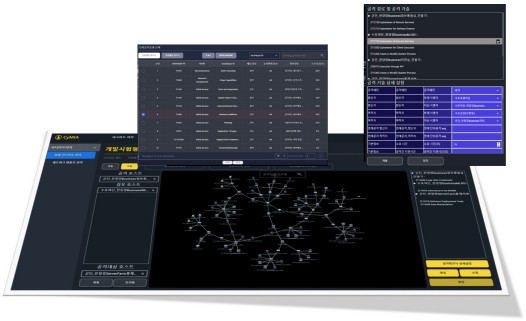
모델종류	수량	비고
자산	28	물리 자산(6), 정보체계 자산(5), 통신체계 자산(6), 방어 자산(11)
과업	10	감시정찰, 정보종합, 지휘결심, 화력지원, 화력운용, 일반과업, 적 이동모의, 적군공격, AND, OR
사이버공격	198	공통패턴(191), 복합패턴(7)

축된 모델을 이용하여 임무환경을 구성하는 임무 시나리오와 사이버공격을 수행하기 위한 사이버공격 시나리오를 저작해야 한다.

그림 11은 임무 시나리오를 저작하는 과정에서 모델간 연계방법의 구현결과를 나타낸 것이다. 임무 시나리오는 임무를 수행하는 과업 모델을 이용하여 저작한다. 과업 모델 속성에서 과업별 운용 자산과 서비스를 자산 모델과 서비스모델을 이용하여 선택한다.

(그림 11) 임무 시나리오 저작시 모델간 연계방법 구현 결과
(Figure 11) Implementation Results of Inter-model Linkage Methods in Mission Scenario Authoring

그림 12는 사이버공격 시나리오 저작시 단위공격 모델 연계방법의 구현결과를 나타낸 것이다. 자산 모델의 취약점을 이용하여 공격 경로와 단위공격 모델을 자동 혹은 수동으로 선택한다. 자동의 경우 최단 경로, 최소 경로, 무작위 공격 별로 공격 경로가 목록으로 제공되는데, 이중 하나를 선택하면 선택된 경로로 호스트별 가능한 단위공격 목록을 자동으로 제시해 준다. 목록 중에서 하나를 선택하면 공격테크닉이 설정이 되며, 상세설정을 통해 사이버공격 시나리오를 완성한다.



(그림 12) 단위공격 모델 연계방법 구현 결과
(Figure 12) Implementation Results of Unit Attack Model Integration Methods

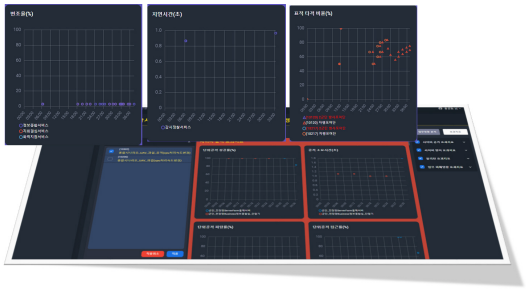
4.3 시뮬레이션 결과로부터 임무피해 산출 구현 결과

CyMIA 도구는 임무피해영향 효과지표로 표 2와 같이 임무계층에서 7종, 과업계층에서 2종, 서비스계층에서 4종, 자산계층에서 6종을 구현하였다. 임무피해영향 효과지표는 사이버공격이 임무에 영향을 주는 요소를 계층별로 선정하였다. 자산계층에서는 기밀성, 무결성, 가용성 측면, 자산간 정보의 전송 성공, 실패 측면, 아군 장비와 부대 피해 측면을 반영하였다. 서비스 계층은 임무파일 변조, 서비스 지연, 서비스 전송 성공여부와 적시성을 반영하였다. 과업계층에서는 과업별 소요시간과 유효시간 내 처리에 따른 성공여부를 반영하였다. 임무는 임무의 완료시간, 성공여부와 임무성공여부를 판단할 수 있는 요소를 반영하였다. 임무피해 효과지표는 매번 산출되는 필수 항목과 임무종류에 따라 산출되는 항목이 있다. 필수 항목은 사이버공격과 직접적으로 관련된 지표이며, 임무종류에 한정된 항목은 임무수행과 연관된 지표이다. 임무종류에 한정된 항목은 수행하는 임무종류에 따라 추가적인 항목 식별이 필요하다. 표 2에 식별된 임무피해 효과지표는 대화력전 임무에 대한 것이다.

임무피해 효과지표는 임무 시나리오와 사이버공격 시나리오의 시뮬레이션 과정에서 자동으로 산출되어 데이터베이스에 저장된다. CyMIA에서 시뮬레이션 결과 목록 중 하나를 선택하면 시뮬레이션 결과를 도시해 주는데 임무피해 효과지표를 선택하여 지표값을 그래프로 확인할 수 있다. 그림 13은 CyMIA에서 제공하는 지표의 일부를 나타낸 것이다.

(표 2) 임무피해 효과지표 구현결과
(Table 2) Implementation Results of the Mission Damage Effect Indicators

계층	임무피해 효과지표	필수여부
임무	완료 소요시간(초)	√
	성공 여부	√
	적 부대 무력화율(%)	
	아군 체계 반응 시간(초)	
	표적 타격 비율(%)	
	사격명령 착오율(%)	
	중복표적 발생률(%)	
과업	과업 소요 시간(초)	√
	성공여부	√
서비스	변조율(%)	√
	지연시간(초)	√
	성공률(%)	√
	적시성	√
자산	변조율(%)	√
	지연시간(초)	√
	성공률(%)	√
	손실률(%)	√
	아군장비 손실률(%)	
	아군부대 피해율(%)	



(그림 13) 임무피해 산출 지표 구현 결과
(Figure 13) Implementation Results of Mission Damage Assessment Metrics

5. 결 론

사이버전에 의한 임무 피해를 정량적으로 산출하기 위해서는 피해평가 모의방법과 모의 내용이 반영된 모델을 개발해야 한다. 사이버공격에 의한 임무체계의 피해를 분석하기 위해서는 자산에서 임무체계까지를 계층별로 분류하고, 계층간 연결관계를 정의한 후 계층간 피해가 전파되는 모델을 개발해야 한다. 본 논문에서는 계층

간 종속관계를 이용하여 사이버공격에 의한 임무체계의 피해를 평가할 수 있는 모델의 모의방법과 M&S 기술을 활용하여 사이버전에 의한 임무 피해평가를 위한 모델을 구현하는 방법을 제안하였다. 또한 제안한 방법에 따라 구현한 모델을 제시하였다.

본 논문에서 제안한 모델은 시범적으로 3종류의 임무체계를 대상으로 검증하였으며, 향후 군의 다양한 임무체계를 대상으로 사이버공격에 의한 임무피해평가를 정량적으로 분석할 것으로 기대된다. 본 연구결과는 민수쪽에서도 활용도가 높을 것으로 판단된다. 전력망, 통신망, 금융 시스템 등 국가의 중요한 기반 시설에 대한 임무보장을 위한 방안 마련에 활용할 수 있을 것이다.

향후 연구방향은 모델의 유효성을 검증하기 위한 다양한 임무체계에 적용하고, 모델의 고도화를 위해 인공지능 및 머신러닝 기술을 접목한 연구를 수행할 예정이다.

참고문헌(Reference)

[1] Wansoo Cho, “The Analysis of Evaluation the Impact of Cyber Attacks on Mission Systems,” Research Report ADDR-412-220103, Agency for Defense Development, 2022.

[2] Yonghyun Kim, Donghwa Kim, Donghwan Lee, Juyoub Kim, Myung Kil Ahn, “Integrated Scenario Authoring Method using Mission Impact Analysis Tool due to Cyber Attacks,” Journal of Internet Computing and Services, Vol. 24, No. 6, pp. 107-117, 2023.
https://doi.org/10.7472/jksii.2023.24.6.107

[3] G. Jakobson, “Mission cyber security situation assessment using impact dependency graphs,” in 14th International Conference on Information Fusion, IEEE, pp. 1-8, 2011.
https://ieeexplore.ieee.org/abstract/document/5977648

[4] X. Sun, A. Singhal, P. Liu, “Towards actionable mission impact assessment in the context of cloud computing,” in IFIP Annual Conference on Data and Applications Security and Privacy,” Springer, pp. 259-274, 2017.
https://doi.org/10.1007/978-3-319-61176-1_14

[5] Salter, C. Saydjari, O. S. Schneider, B., “Toward a Secure System Engineering Methodology,” in NSPW’98, Proceedings of the 1998 Workshop on New Security Paradigms, 1998.
https://dl.acm.org/doi/pdf/10.1145/310889.310900

[6] Jajodia, S. Noel, S., “Topological Vulnerability Analysis,” Cyber Situational Awareness Advances in Information Security, Vol. 46, pp 139-154, 2010.
https://doi.org/10.1007/978-1-4419-0140-8_7

[7] S. Musman, A. Temin, M. Tanner, R. Fox, B. Pridemore, “Evaluating the Impact of Cyber Attacks on Missions,” in Proceeedings of the 5th International Conference on Information Warfare and Security, Dayton, Ohio, 2010, edited by E. Armistead and E. Cowan, pp. 446-456, 2010.

[8] Alexandre, B., Paulo, C., Michael, H., “Cyber-Argus: Modeling C2 Impacts of Cyber Attacks,” 19th ICCRTS -C2 Agility: Lessons Learned from Research and Operations, 2014.
https://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/5512e918e4b007aba5c466db/1427302680975/2014-096p.pdf

[9] Kaixing, H., Chunjie, Z., Yu-Chu, T., “Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems,” IEEE Transactions on Industrial Electronics, Vol. 65 Issue 10, pp. 8153-8162, 2018.
https://doi.org/10.1109/TIE.2018.2798605

[10] Noel, Steven, et al., “Analyzing mission impacts of cyber actions (AMICA),” INATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact, pp. 80-86, 2015.
https://apps.dtic.mil/sti/pdfs/AD1000707.pdf#page=86

[11] S. Musman and A. Temin, “A Cyber Mission Impact Assessment Tool,” IEEE International Symposium on Technologies for Homeland Security, pp 1-7, 2015.
https://doi.org/10.1109/THS.2015.7225283

[12] Melanie Bernier, “Military Activities and Cyber Effects(MACE) Taxonomy,” DefenceR&D Canada, 2013.

[13] K. C. Kapur and L. Lamberson, Reliability in engineering design, New York, 1977

[14] Yonghyun Kim, Donghwa Kim, Donghwan Lee, Juyoub Kim, Miyoung Kwon, Myungkil Ahn, “Implementation of Mission Damage Assessment Model due to Cyber Attacks,” 2024 Korea Society Internet Information Spring Conference, pp. 103-104, 2024.

◐ 저 자 소 개 ◑

김 용 현(Yonghyun Kim)
1993년 광운대학교 전자공학과(공학사)
1995년 광운대학교 대학원 전자공학과(공학석사)
2013년 광운대학교 대학원 전자통신공학과(공학박사)
1995년~현재 국방과학연구소 수석연구원
관심분야 : 사이버보안, 무선센서네트워크 etc.
E-mail : yonghyunkim@add.re.kr

김 동 화(Donghwa Kim)
2004년 고려대학교 전기전자전파학과(공학사)
2007년 고려대학교 대학원 전기공학과(공학석사)
2024년 세종대학교 대학원 컴퓨터공학과(공학박사)
2007년~현재 국방과학연구소 책임연구원
관심분야 : 사이버보안, 사이버전 M&S etc.
E-mail : dhkim@add.re.kr

이 동 환(Donghwan Lee)
2006년 고려대학교 산업시스템정보공학과(공학사)
2008년 고려대학교 컴퓨터학과(이학석사)
2008년~현재 국방과학연구소 선임원구원
관심분야 : 무선네트워크 보안, 분산시스템 보안, 사이버전 M&S 등
E-mail : dlee@add.re.kr

김 주 엽(Juyoub Kim)
1992년 경기대학교 경영정보학과(경영학사)
1995년 서강대학교 대학원 경영학과(경영석사)
1995년~현재 국방과학연구소 책임연구원
관심분야 : 사이버보안, 센서네트워크 etc
E-mail : pluto@add.re.kr

권 미 영(Miyoung Kwon)
1987년 이화여자대학교 전산학과(이학사)
1992년 고려대학교 경영대학원 경영학과(경영학석사)
1988년~현재 국방과학연구소 수석연구원
관심분야 : 사이버보안, 센서네트워크 etc
E-mail : kmyadd@add.re.kr

안 명 길(Myung Kil Ahn)
1997년 충남대학교 정보통신공학과(공학사)
2003년 서강대학교 대학원 컴퓨터공학과(공학석사)
2021년 중앙대학교 대학원 전자전기공학과 컴퓨터전공(공학박사)
2006년~현재 국방과학연구소 책임연구원
관심분야 : 사이버보안, 사전위협분석 및 취약성검증
E-mail : happyahn@add.re.kr