Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.2, Apr. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.2.533

사이버전사의 훈련을 위한 시스템 구축 방안 연구

안 명 길,† 김 용 현‡
국방과학연구소

Research on System Architecture and Simulation Environment for Cyber Warrior Training

Myung Kil Ahn,† Yong Hyun Kim‡
Agency for Defense Development(ADD)

요 약

급증하는 사이버 위협에 능동적으로 대응하기 위해, 사이버전사의 훈련, 기술검증 지원, 전투실험 임무는 매우 중요하다. 하지만, 실 운용 망에서 이를 수행하는 것은 많은 제약이 따르므로, 평상시 끊임없이 수행하기 위한 환경 및 시스템 구축이 필요하다.

본 논문에서는 사이버전사의 훈련 및 기술검증 지원을 위해 실(live)/가상(virtual) M&S 기반의 시스템 및 기능을 제안하고, 전투실험을 위해 구성(constructive) M&S 기반의 시스템 및 기능을 제안한다. 실제와 유사한 환경에서 다양한 시나리오를 기반으로 훈련을 수행함으로써 사이버전에 대한 사이버전사의 역량을 강화하고, 대규모 전장 환경의 사이버 위협에 대한 피해 영향을 사전에 분석함으로서 대응책 마련에 유용하게 활용가능하다.

ABSTRACT

It is important to establish the environment for cyber warrior training, testing support and effectiveness analysis in order to cope with sharply increasing cyber threat. However, those practices cannot be easily performed in real world and are followed with many constraints.

In this paper, we propose a live/virtual M&S-based system for training/testing and constructive M&S-based system for effectiveness analysis to provide an environment similar to real world. These can be utilized to strengthen the capability to carry out cyber war and analyze the impact of cyber threat under the large-scale networks.

Keywords: Cyber training, Modeling&Simulation, Cyber effectiveness analysis, Cyber warfare

I. 서 론

사이버전은 핵전과 비유되는 비대칭 전쟁방식의 하나로 육, 해, 공, 우주에 이은 제 5의 전장으로 인식되고 있다. 단순히 정보보호 수준을 넘어 정보체계 및 무기체계에도 영향을 미치며, 궁극적으로 군의 전략/작전 수행에 결정적 영향을 줄 수 있다. 이에 사이버전을 대비하고 능동적으로 대응하기 위해, 평소 끊임없이 훈련하고, 다양한 시나리오를 기반으로 사이버전 전투 실험 및 피해에 대한 효과분석을 수행해야 한다. 하지만, 실 운용 망을 대상으로 이를 수행하는 것은 큰 위험 부담 및 제약이 발생하며, 현실적으로 불가능하다.

미국 등 선진국에서는 사이버전의 수행능력을 높이기 위해 많은 노력을 기울이고 있으며, 특히 미국 DARPA(Defense Advanced Research Projects Agency)에서는 국가사이버전 시험장 (NCR, National Cyber Range)[1][2]을 개발하여, 사이버

Received(02 .22. 2016), Modified(03. 25. 2016), Accepted(03. 28. 2016)
† 주저자, lovedew123@gmail.com
‡ 교신저자, yonghyun99@empal.com(Corresponding author)

전 훈련 및 시험을 위한 테스트베드를 지원한다.

우리 군도 전평시 구분없이 사이버전에 대비하기 위해, 다양한 환경 및 시나리오를 기반으로 사이버전 훈련을 수행하고, 신규 사이버 기술에 대한 시험검증을 지원하고, 대규모 군 통신망에 대한 사이버전 실험분석을 통해 위협 발생 시 피해분석 및 대응책을 확보하기 위한 방안을 검토 중에 있다. 이를 수행하기 위한 환경 구축을 위해 M&S(Modeling& Simulation) 기술 활용은 필수적이다.

본 논문에서는 사이버전 훈련, 기술검증, 전투실험 수행을 위한 사이버전 모의 환경 구축 방안을 제시하고, 이를 기반으로 사이버전을 대비한 사이버전사의 훈련 및 임무 역할에 대해 제안하고자 한다.

본 논문의 구성은 II장에서 사이버전사 훈련 시스템 구축에 필요한 관련 기술 연구를 살펴보고, III장에서 사이버전 훈련 및 기술검증에 대한 시스템 구성 및 기능을 제안한다. IV장에서는 사이버전 전투실험에 대한 시스템 구성 및 기능을 제안하고, V장에서 결론을 맺는다.

II. 관련 연구

실제와 유사한 상황에서 사이버전사의 훈련, 기술검증, 전투실험 임무를 수행하기 위해, 실세계를 정확하고 활용목적에 맞게 모의하는 것이 중요하다. 실세계는 제반환경, 행위, 사람, 장비, 프로세스 등을 의미하며, 이에 대해 모델화하고 시간의 흐름에 따라 구동되도록 한다. 이러한 M&S 기술은 국방 분야에서 주요기술로 식별되고 있으며, 본 논문의 사이버전 모의 환경 구축을 위해 활용된다.

국방 M&S의 개념 및 분류에 대해 정리하고, 가상환경 구축을 위해 필수적인 가상화 기술, 구성환경 구축을 위해 필수적인 Cyber Effect 모델에 대해 설명한다.

2.1 국방 M&S

국방분야 M&S는 임무계획 수립을 위한 수행연습 및 효과분석, 사용자 훈련, 기술개발 및 시험검증, 획득 목적을 위해 다양하게 활용되고 있다. 국방 M&S는 Fig.1.과 같이 분류될 수 있다[3].

실제 사람이 실제 시스템을 기반으로 수행하는 것은 실(live)환경, 실제 사람이 가상 시스템을 기반으로 수행하는 것은 가상(virtual)환경, 가상의 사람

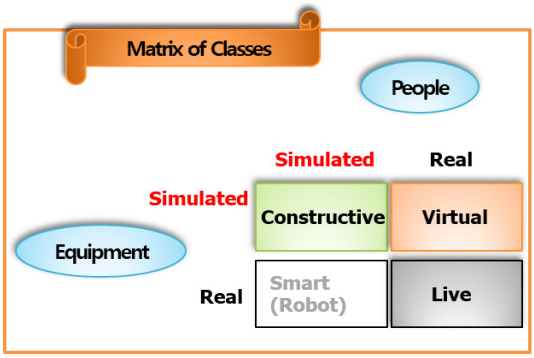

Fig. 1. Matrix of Classes of Models and Simulations

이 가상의 시스템을 기반으로 수행하는 것은 구성(constructive)환경으로 분류한다. 실환경은 실제와 같은 사이버전 환경을 제공할 수 있으나, 제원이 한정되어 있어 규모면에서 제약이 따른다. 또한 시나리오 반복 및 재연이 불가하다. 가상환경은 실제와 유사한 사이버전 환경을 제공하면서, 실환경에 비해 제원에 대한 제약이 덜한 장점이 있다. 그러나, 거대규모의 사이버 전장 환경을 구성하기에는 무리가 있다. 구성환경은 실환경 및 가상환경에 비해 제원에 대한 제약이 덜해 대규모 환경을 구성할 수 있는 장점이 있으나, 정확도(fidelity) 및 해상도(resolution)를 높이기 위한 많은 노력이 필요하다.

2.2 가상화 기술

사이버전사의 훈련 및 기술검증 지원 수행을 위해 실/가상 M&S 환경을 구축하며, 호스트 기반의 가상화 기술 및 네트워크 가상화 기술을 활용하여 구성이 가능하다.

호스트 기반의 가상화 기술은 하드웨어를 가상화하는 것으로 CPU, 메모리, 하드디스크, 네트워크 카드 등과 같이 실제 하드웨어를 모방하여 가상의 컴퓨터인 가상머신을 만드는 것이다. 네트워크 가상화 기술은 스위치, 라우터, 방화벽 등에 대한 가상화 솔루션을 제공하며, 이를 이용하여 수십 대에서 수백 대의 호스트를 이용한 가상 네트워크를 구성할 수 있다[4]. 호스트 가상화 및 네트워크 가상화는 VMWare와 같은 가상화 솔루션을 이용해 구축할 수 있다.

특히, 국방 분야에서는 무기체계 대상의 사이버 위협에 대비하기 위해, 무기체계 내장형 OS/SW에

대한 가상화 플랫폼 기술 관련 연구를 추진 중에 있다.

2.3 Cyber Effect 모델

미 국방정보체계국(DISA, Defense Information System Agency)에서는 군통신망 분석 및 계획수립을 위해, Riverbed Modeler(구, OPNET Modeler) 기반의 통신망 M&S 분석도구인 JCSS(Joint Communication Simulation System)를 개발하여 운용 중에 있다[5].

또한, 우리 군에서도 Riverbed Modeler 기반으로 군 통신환경을 모의하고 정보교환 적시성 분석이 가능한 NetSPIN(Network Simulator& Planner for INteroperability)을 개발 완료하여 활용 중에 있다.

Riverbed Modeler는 높은 시장 점유율을 보유한 상용 네트워크 시뮬레이션 툴로서, 검증된 시뮬레이션 엔진과 방대한 표준장비 모델을 제공하고 있으며, 최근 사이버 위협에 미치는 양상을 모의하기 위해 Cyber Effect 모델을 제공하고 있다[6].

기존의 특정 사이버 위협만을 모델링하거나 실제 사이버 공격코드를 이용하는 제한적인 방법이 아닌, 사이버 위협에 대한 효과 기반으로 계층 구조의 위협 시나리오를 모델링할 수 있는 방안을 제시한다. 사이버 위협은 하나의 Profile로 모의되며, 내부는 여러 개의 Phase-Script로 구성된다.

Fig.2.에서 Phase는 하나의 Script를 포함하나 Script는 여러개의 Phase에서 재사용될 수 있다. Script는 하나 이상의 Effet를 포함하며, 사이버 위협에 대한 효과를 명시한다.

이를 활용하여 대규모 네트워크 모의 환경에서, Cyber Effect 모델 기반 다양한 사이버 위협을 모델링하고[7], 위협으로 인해 발생하는 피해분석 및 대응 방책(Course of Action)을 모색하는데 활용할 수 있다.

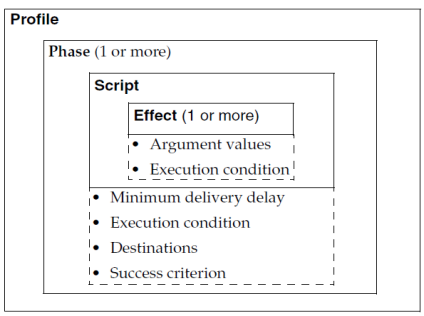

Fig. 2. Anatomy of a Cyber Profile

III. 사이버전 훈련 및 기술검증

사이버전사의 훈련 및 기술검증을 위해, 실환경과 가상환경을 기반으로 시스템을 구축한다. 다양한 시나리오를 기반으로 사이버전 훈련을 수행하고, 신규 사이버 위협에 대한 검증을 수행할 수 있다.

3.1 시스템 구성

사이버전 훈련 및 기술검증을 위한 환경은 보다 정확하고 실제와 유사한 훈련 및 세밀한 검증이 가능하도록, 실장비 및 가상화 기술을 활용한 가상장비로 Fig.3.과 같이 구성될 수 있다.

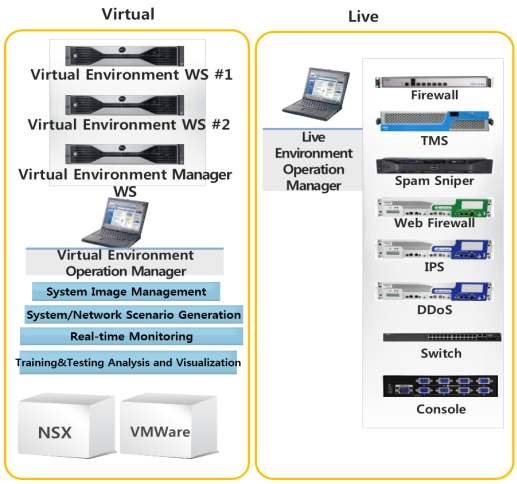

Fig. 3. System Configuration of Live/Virtual environment

실환경은 방화벽, 웹방화벽, 침입방지시스템 등과 같은 실제 보안장비를 활용하여 구성하고, 가상환경은 호스트 가상화 및 네트워크 가상화 기술을 활용하여 가상장비로 구성한다.

3.2 시스템 기능

사이버전 훈련 및 기술검증 수행을 위해, 시나리오 생성, 일반/위협트래픽 발생, 환경통합 모니터링,

결과분석을 위한 로그수집 및 가시화 기능으로 구성된다.

먼저, 다양한 사이버전 상황에서 훈련 및 기술검증을 수행할 수 있도록, 각 목적에 맞게 Fig.4.와 같이 시나리오를 생성할 수 있다. 가상환경에서는 OS(Windows 계열, LINUX 등), 웹/메일/DNS/데이터베이스, 시스템/네트워크장비 등이 이미지형태로 관리되며, 시나리오 저작자가 편리하게 작업할 수 있도록 GUI(Graphic User Interface)를 통해 Drag&Drop 방식으로 시나리오 생성이 가능하도록 한다. 가상이미지는 구동, 정지, 재시작, 정보확인 등이 가능하며, 가상이미지를 배치 및 연결하고, 구성정보를 설정하여 시나리오를 생성한다. 실장비도 동일 시나리오에 배치하여 저작이 가능하다.

실제와 유사한 사이버전 상황에서 훈련이 진행될 수 있도록, 또한 다양한 사이버전 환경에서 기술검증을 수행할 수 있도록, 일상적으로 발생하는 정상행위 및 위협행위가 발생이 되어야 한다.

일상적으로 발생하는 정상행위는 웹, 메일, 자료연동체계를 통한 자료연동 행위 등을 말한다. 실제 사람이 발생시키거나, 확률분포 및 모수값 설정에 따라 사람의 행위를 모의하여 정상행위를 수행할 수 있으며, 이러한 정상행위를 통해 일반트래픽이 발생된다.

웹 행위를 모사하는 경우 Fig.5.와 같이 설정할 수 있다. 웹 행위에 대한 설정값을 입력받아 확률분포 기반 정상 웹 행위를 모사한다. 접속 URL 목록, URL별 재귀적 방문 횟수, URL 접속 주기 등의 설정값을 입력받고, 이를 기반으로 URL 접속 행위, 하이퍼링크 클릭행위, 뒤로가기 행위 등을 수행한다.

위협행위의 경우 훈련 및 기술검증 목적으로 일반 상용 모의침투도구를 활용하여 위협을 발생시키거나, 위협 스크립트를 탑재한 이미지를 구동시킬 수 있다.

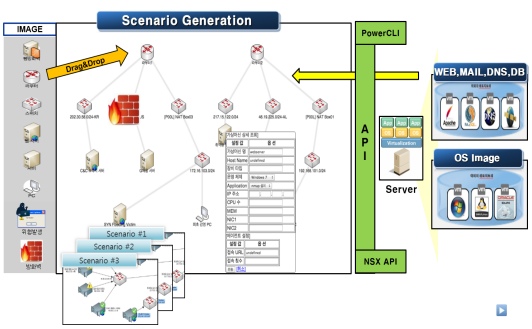

Fig. 4. Concept of Scenario Generation

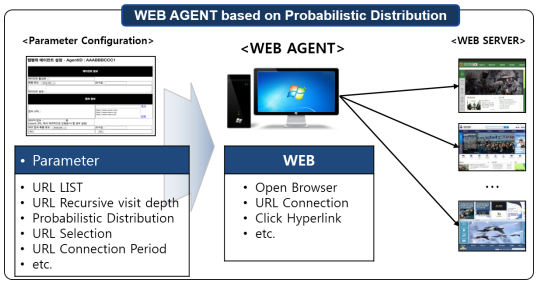

Fig. 5. Parameter of Web Agent

사이버전 훈련 및 기술검증 시, 실시간 이벤트에 대한 발생 및 처리현황을 편리하게 관제운영하기 위한 환경통합 모니터링 대시보드가 구성된다.

또한, 가상머신의 자원 사용율(CPU, 메모리, DISK 등)을 수집하여 호스트 자원에 대한 정보를 제공하고, 위협/방어 행위를 수집하여 이벤트 발생 시 알람을 발생하고, 사용자가 편리하게 결과 데이터를 분석 및 활용할 수 있도록 목록형태 및 그래프형태로 가시화하여 제공한다.

3.3 사이버전 훈련 시스템 구축 예시

사이버전사의 사이버전 훈련을 위해, Fig.6.과 같이 시스템을 구성할 수 있다.

관리자인 White Team은 훈련 목적에 따른 시나리오를 저작하고, 대항군 목적의 공격훈련자인 Red Team과 방어훈련자인 Blue Team에게 각 할당된 공격/방어장비에 대한 제어 권한을 부여하고, 공격/방어 훈련에 대한 임무를 전달한다. 공격훈련자와 방어훈련자는 기본적으로 공격도구 및 방어장비를 사용하고, 각 훈련자의 역량에 따라 다양하게 임무를 수행할 수 있다.

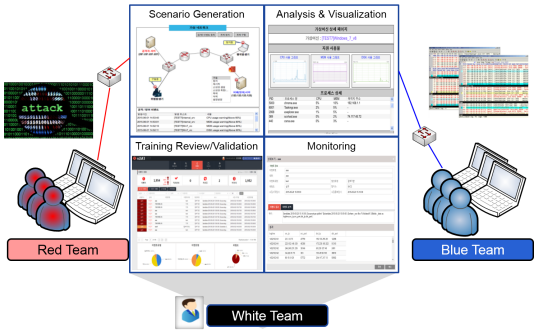

Fig. 6. Concept of Cyber Training

공격 훈련시, 관리자는 시나리오 저작을 통해 방어장비를 배치하고, 훈련자는 시나리오를 기반으로 각 단말에서 대항군 임무를 수행한다.

방어 훈련시, 관리자는 방어훈련자 대상 공격생성을 위해 공격도구 및 가상화된 공격이미지를 구동하여 공격을 생성한다. 방어훈련자는 방어장비 등을 활용하여 방어임무를 수행한다.

공방 훈련시, 관리자는 사이버전 환경을 구축하고 공방에 대한 전반적인 상황을 모니터링하고 평가한다. 공격훈련자는 각 단말에서 공격 임무를 수행하고, 방어훈련자는 방어장비 등을 활용하여 방어임무를 수행한다.

3.4 사이버전사의 역할 및 활용방안

본 사이버전 훈련 시스템을 기반으로 사이버전사의 훈련 및 기술검증 임무를 수행할 수 있으며, 군 특수 목적의 훈련 시나리오 및 보안기술, 컨텐츠 등이 탑재될 수 있다. 또한 적성국의 주요 프로그램을 확보 설치하여 분석 및 이에 대한 대응 훈련을 수행할 수 있다.

더불어, 무기체계 가상화 연구가 완료되면, 민간에서 수행할 수 없는 무기체계 기반 훈련 환경을 구축하여 감시정찰, 사이버 지휘통제 등 실전적 사이버 전투 훈련 연습이 가능할 것이다.

IV. 사이버전 전투실험

사이버전사의 전투실험 수행을 위해, 구성 M&S 환경을 기반으로 시스템을 구축한다. 대규모 군 전장 환경을 모의하고, 다양한 사이버전 시나리오를 적용하여, 위협에 따른 피해 효과분석 및 대응책을 확보하는 능동적인 사이버전 대응을 수행할 수 있다.

4.1 시스템 구성

사이버전 전투실험을 위한 환경은 대규모 전장 환경을 구성해야 하므로, 실장비나 가상장비를 활용하여 규모면으로 동일하게 구성하는 것은 한계가 있다. 사이버 효과를 반영한 대규모 시스템 및 네트워크 장비 모의를 위해, Cyber Effect 모듈을 탑재한 Riverbed Modeler를 활용하여, 정밀한 공학급 수준의 전투실험 구성모의환경을 구축한다.

시스템 구성은 Fig.7.과 같으며, 이산사건 시뮬레이션(DES, Discrete Event Simulation) 엔진을 기반으로 사이버전 환경을 모의한다.

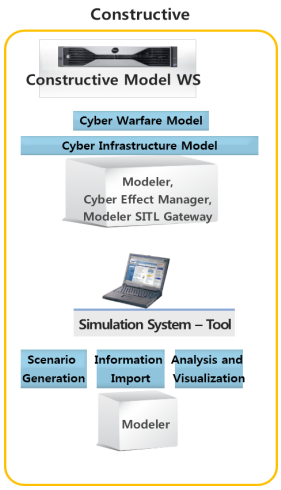

Fig. 7. System Configuration of Constructive environment

4.2 시스템 기능

사이버전사의 전투실험 수행을 위한 운용절차는 Fig.8.과 같다. 전투실험 시나리오 생성을 위해 시스템 및 네트워크 장비를 배치하고, 필요한 정보를 입력한다. 분석을 원하는 사이버 위협 및 방어 시나리오를 저작하고 시뮬레이션을 실행한다. 시뮬레이션이 종료되면 결과에 대한 분석을 수행한다.

사이버전 전투실험을 위해, 사이버전 운용환경모델, 사이버전 모델이 구현되어야 하며, 이를 기반으로 시나리오 저작, 효과분석 및 가시화 기능이 수행된다.

사이버전 운용환경모델은 전투실험이 수행되는 군 전장 환경을 의미하며, 사이버 효과를 반영할 수 있도록 시스템 및 네트워크 장비가 모의된다. 시스템 장비는 CPE(Common Platform Enumeration)을 활용하여 모의하며, 시스템에 설치되는 운영체제의 종류 및 버전, 설치된 응용/서비스 종류 및 버전

Fig. 8. Process of Cyber Warfare experimentation

등을 포함한다. 일반 상용 장비 외에 군 통신 GOTS (Government Off The Shelf) 장비들이 모의된다. 또한 CPU와 메모리의 주요 제원을 모의한다.

사이버전 모델은 실제 위협을 발생시키는 사이버 위협 모델 및 방어 장비를 의미한다.

사이버 위협 모델은 최종 목적을 달성하기 위한 효과(effect)기반의 단위 위협(phase)들의 조합 형태로 Fig.9.와 같이 구성된다.

사이버 위협에 대한 효과는 IETF Extended Incident Handling(INCH) Working Group에서 발표한 침해지표 규약인 IODEF(Incident Object Description and Exchange Format)[8]을 기반으로 하며, 사이버 위협에 의해 시스템 및 네트워크에 미치는 영향으로 Table 1.과 같이 분류된다.

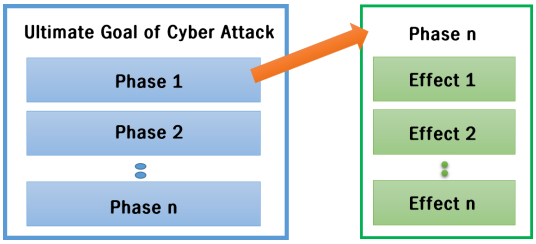

Fig. 9. Concept of Cyber Attack Modeling

Table 1. Malicious Activity Classification

Type	Description
admin	Administrative privileges were attempted
dos	A denial of service was attempted
file	An action that impacts the integrity of a file or database was attempted
info-leak	An attempt was made to exfiltrate information
misconfiguration	An attempt was made to exploit a mis-configuration in a system
policy	Activity violating site's policy was attempted
recon	Reconnaissance activity was attempted
social-engineering	A social engineering attack was attempted
user	User privileges were attempted
unknown	The classification of this activity is unknown

사이버전 운용환경 모델과 사이버전 모델을 기반으로 전장망 구성 및 사이버전 공방 시나리오를 저작한다. 특정 혹은 다수의 위협을 선정하고, 공격 목표 및 대상을 지정한다. 취약점 DB를 기반으로 대상 공격목표가 사이버 위협에 대해 취약한 지를 확인한 후 사이버 공격 절차가 진행된다. 배치된 다수의 방어 장비가 시나리오에 따라 구동되며, 사이버전 공방 시나리오가 전개된다.

대규모 군 전장 환경에서 적의 사이버 공격이 발생할 경우, 또는 민간에서 발생한 사이버 공격에 대해 군 상황에 적용 시, 위협에 따른 피해 효과분석이 수행된다.

위협에 대한 감염/전파율, 감염 차단 등의 방어 능력, 자원 소진률, 정보교환의 적시성(timeliness) 영향력, 기밀성, 가용성 등 다양한 관점의 지표산출을 통해 효과를 분석함으로서, 군의 사이버 방어 능력 향상 및 대응책 마련에 활용할 수 있다.

4.3 사이버전 전투실험 예시

군 C4I(Command, Control, Communication and Intelligence)체계는 기반체계와 전장관리체계로 구성되며, 민간 상용 장비 외에 군 전용 통신장비들이 배치된다. 본 논문에서 제시한 사이버전 전투실험 환경을 기반으로, 대규모 군 전장 통신 환경을 구축할 수 있다. 사이버 전사는 민간발생 위협 및 군 특수 위협, 또는 향후 발생 가능한 위협 등 다양한 관점에서 시나리오를 작성하고 전투실험을 수행할 수 있다.

여러 지표 중 적시성 관점에서 피해 효과분석을 수행할 경우, 분석 대상 군 전장 환경을 기반으로 새로운 사이버 위협을 저작하고 적시성 분석지표를 설정한다. 사이버전 공방 시나리오에 따라 시뮬레이션이 수행되며, 적시성에 대한 피해 효과분석 결과가

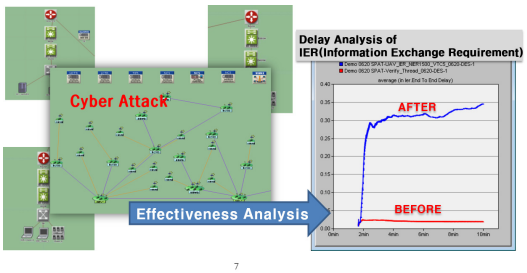

Fig.10. Example of Cyber Effectiveness Analysis

도출된다.

Fig.10.은 예시로 부대 편제 구조에 따른 전장관리체계 대상 DDoS 및 오류 데이터 전달에 의한 정보 교란 공격이 발생할 경우의 시나리오이다. 트래픽 부하로 인하여 노드 종단 간 적시에 도달되어야 할 정보교환요구목록(IER, Information Exchange Requirements)이 전달 지연이 발생하게 되어 적시성을 만족하지 못하게 된다.

4.4 사이버전사의 역할 및 활용방안

본 시스템을 기반으로 사이버전사의 전투실험 임무를 수행할 수 있으며, 대규모 군 통신망에 대한 위협 피해분석을 통해 취약성을 분석하고, 이에 대한 대응 방책(course of action)을 수립하는데 활용될 수 있다.

또한 사이버전사는 사이버공간에서의 작전수행을 위한 사이버 작전 개념과 사이버작전수행 부대 조직 편성, 무기체계 및 장비의 개발을 위한 분석에 본 시스템을 활용할 수 있다.

V. 결 론

사이버전은 전평시 구분없이 매사 대비태세를 갖추어야 한다. 이를 위해 사이버전사의 훈련, 기술검증 지원, 전투실험은 매우 중요하며, 상시 진행될 수 있도록 시스템이 구축되어야 한다.

본 논문에서는 실제와 유사한 환경에서 다양한 시나리오를 기반으로 사이버전사의 훈련 및 기술검증 지원을 수행할 수 있도록 훈련/검증 시스템을 제안하였다. 또한 대규모 전장 환경을 기반으로 사이버전에 대한 피해 효과를 사전에 분석하고 대응책을 마련할 수 있도록 효과분석 시스템을 제안하였다.

제시한 시스템은 사이버전사의 교육훈련 및 양성에 유용하게 활용될 수 있으며, 사이버전 대응을 위한 다양한 시나리오 개발에 활용될 것으로 기대된다.

References

[1] R. Hollister, P. Lardieri, and L. Pridmore, "National cyber range(NCR) automated test tools: implications and application to network-centric support tools," IEEE Conference, AUTOTESTCON, pp. 1-4, Sept. 2010

[2] B. Ferguson, A. Tall, and D. Olsen, "National cyber range overview," IEEE Military Communications Conference, pp. 123-128, Oct. 2014

[3] Michael V. R. Johnson, Mark F. McKeon, and Terence R. Szanto, "Simulation based acquisition: a new approach," DSMC, Dec. 1998

[4] KIM HYUK JOON, Donghwan Lee, Myung Kil Ahn, Yong-Hyun Kim, and Ki-Seong Noh, "Measuring technical effectiveness in cyber warfare," Korea Computer Congress, pp. 143-145, June 2015

[5] DISA, https://www.disa.mil/Mission-Support/ Enterprise-Engineering/JCSS

[6] Riverbed Modeler, http://www.riverbed.com/products/performance-management-control/opnet.html

[7] Myung Kil Ahn, DongHwan Lee, Donghwa Kim, and Yong Hyun Kim, "Research on method of cyber attack modeling in constructive M&S network environment," The Fall Conference of the KIMST, pp. 773-774, Nov. 2015

[8] eCSIRT, IODEF/IMDEF Solutions, http://www.ecsirt.net/service/products.html

〈저자소개〉

안 명 길 (Myung Kil Ahn) 정회원
1997년: 충남대학교 정보통신공학과 졸업
2003년: 서강대학교 컴퓨터공학과 석사
2016년: 중앙대학교 전자공학과 박사과정
1997년~2006년: LG전자 정보통신 연구소
2006년~현재: 국방과학연구소 선임연구원
〈관심분야〉 정보보호, 사이버전M&S, 사이버 시뮬라전, 효과분석, 훈련체계

김 용 현 (Yong Hyun Kim) 정회원
1993년: 광운대학교 전자공학과 졸업
1995년: 광운대학교 전자공학과 석사
2013년: 광운대학교 전자통신공학과 박사
1995년~현재: 국방과학연구소 책임연구원
〈관심분야〉 사이버 시뮬라전, 배틀랩 구축, WSN, 사이버전 M&S, 훈련체계