정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

가상 개발환경 기반의 차량용 사이버훈련 프레임워크 설계: 공격 중심으로

조 영 복*, 최 수 빈*, 오 병 윤*, 김 호 준*, 최 영 호*, 정 성 훈**, 곽 병 일***, 한 미 란*

요 약

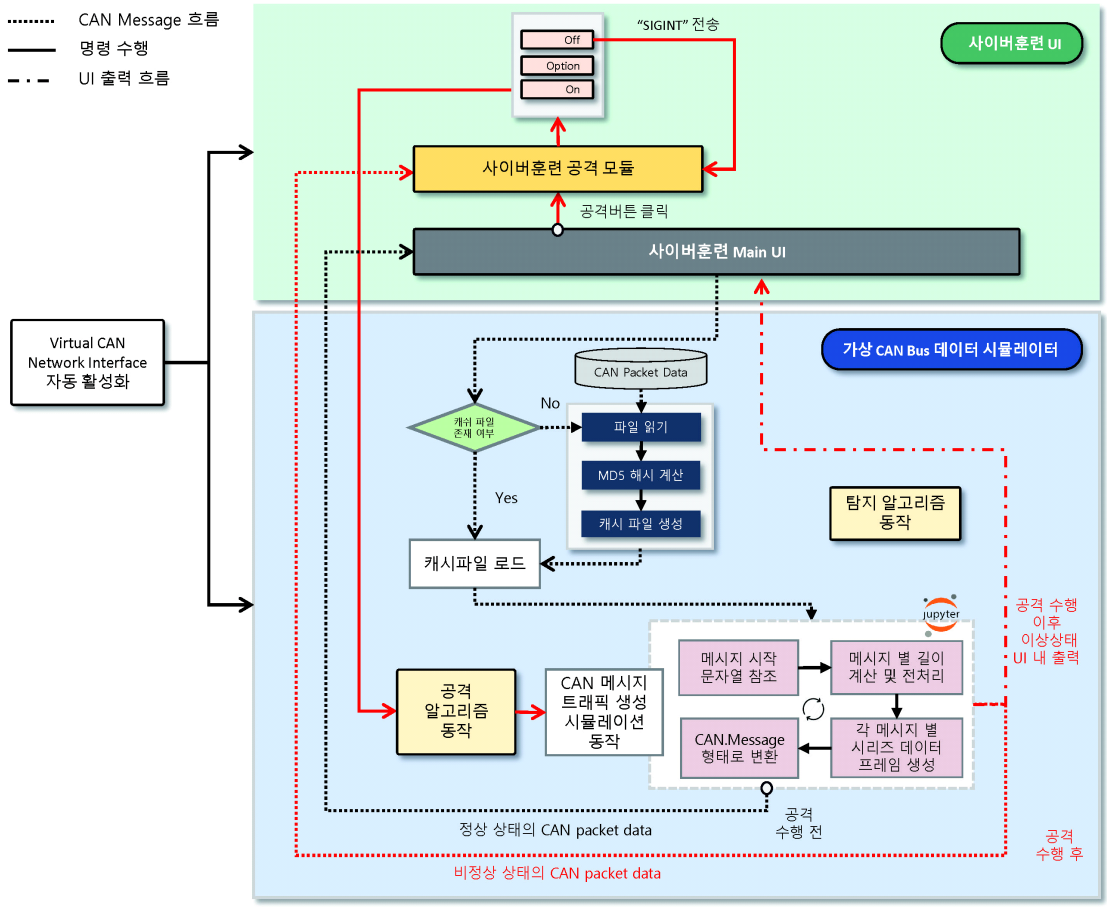
대부분의 임베디드 시스템은 기계장치와 전자기기 장치가 함께 작동되는 물리 장치로써, 이기종 네트워크, 복잡한 보안체계 등을 고려하여 가상화 기반 사이버훈련 환경이 구성되어야 한다. 또한, 차량을 대상으로 물리적인 실험 환경에서 모의침투 등 사이버훈련을 수행한다는 것은 교통사고를 비롯한 안전사고 발생에 있어 위험이 존재한다. 본 논문에서는 가상 개발환경에서의 공격 기반 차량용 사이버훈련 프레임워크를 제안하고자 한다. 먼저, 공격 기반 차량용 사이버훈련 프레임워크의 작동은 자동 활성화되는 가상의 CAN 네트워크 인터페이스로 시작된다. 가상의 CAN 네트워크 인터페이스는 가상머신에서 간단한 부트스트랩 명령어 실행을 통해 파이썬 패키지와 Ubuntu 서비스 목록 설치 명령이 자동으로 실행되면서 설치된다. 이후 내부 네트워크 시뮬레이터와 공격모듈과 관련된 UI가 자동으로 Ubuntu Systemd에 의해 백그라운드에서 실행되어 시작과 동시에 준비 상태를 유지하게 된다. 사이버훈련 UI 내 공격 모듈은 사용자에 의한 공격 선택 및 파라미터 셋팅 이후 차량의 이상 상태를 사이버훈련 UI에 다시 출력되게 된다. 본 논문에서 제안하는 가상 개발환경 기반의 차량용 사이버훈련 프레임워크는 자율주행 차량 사고의 위험이나 다른 특수한 제약 없이 사용자의 학습 경험을 확장 시킬 수 있다. 또한, 기존의 가상화 기반 사이버훈련 교육 콘텐츠와는 달리 일반 사용자들이 접근하기 쉬운 형태로 확장 개발이 가능하다.

Ⅰ. 서 론

ICT 기술의 발전에 따라 APT (Advanced Persistent Threat) 공격과 같은 지능형 사이버 공격이 더욱 고도화되고 다양화되고 있으며, 해당 공격의 빈도수도 증가하는 추세이다. 이러한 공격에 대응하기 위해 사이버 보안 산업 전반에서 단계적이고 점진적인 보안 인력풀의 확대와 역량 강화에 노력을 기울이고 있다. 이와 더불어, 보안전문가 외 일반인들도 사이버 보안 위협을 빠르게 인지하고 대비하기 위한 사이버훈련 교육 프로그램 개발의 필요성도 대두되고 있다. 최근 한국인터넷진흥원은 정보보호 산업현장 및 서비스에 즉시 투입 가능한 인력양성을 목표로 인터넷침해사고 대응 실전훈련을 위한 실전형 사이버훈련장인 Security-Gym을 운영 중이다[1]. 그리고, 국가정보보안교육원의 사이버안전훈련센터는 정부 부처와 공공기관을 대상으로 보안 교육을 진행하고 있다[2]. 국외의 경우, 이스라엘 사이버 시큐리티 기업인 Cybergym은 보안전문가 뿐만 아니라 비전문가까지도 사이버 보안 교육을 받을 수 있는 과정을 제공하고 있으며, Cybergym과 마찬가지로 미국의 Raytheon Code Center에서는 사이버 공격과 방어에 대한 핵심 기술을 훈련할 수 있도록 지원하고 있다[3,4]. 그러나, 커넥티드 카(Connected Car)와 자율차량과 같은 임베디드 시스템은 기계장치와 전자기기 장치가 함께 작동되는 물리 장치이기 때문에, 이기종 네트워크, 복잡한 보안체계 등을 고려하여 가상화 기반 사이버훈련 환경이 구성되어야 한다. 또한, 차량을 대상으로 물리적인 실험 환경에서 모의침투 등 사이버훈련을 수행할 경우, 교통사고를 비롯한 안전사고 발생의 위험이 존재하므로

“본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원 사업의 연구결과로 수행되었음” (IITP-2023-RS-2022-00164800*) 또한, 이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2021-0-00903, 고신뢰 온-디바이스 딥러닝 가속기 설계를 위한 물리채널 기반 취약점 검증 및 대응기술 개발)

* 고려대학교 과학기술대학 인공지능사이버보안학과 (학부생, {elluardxii12, subin0630, oby0442, wkdwhdkdy100, dudghchl000}@korea.ac.kr, 조교수, blosst@korea.ac.kr)
** 고려대학교 정보보호연구원 (박사후연구원, seonghoon@korea.ac.kr)
*** 한림대학교 정보과학대학 소프트웨어학부 (조교수, kwacka12@hallym.ac.kr)



〔그림 1〕 가상화기반 사이버훈련 프레임워크 (전체 구성도)

가상화 기반 사이버훈련 시스템 도입이 필요하다.

본 논문은 가상화 개발환경의 체계적인 구성과 차량 내부 네트워크에 발생 가능한 공격 유형별 환경 설계에 대해 자세히 다루고 있다. II 장에서는 관련 연구에 대해 살펴보고, III 장에서는 가상 CAN 네트워크 인터페이스 자동활성화와 차량 내부 네트워크 시뮬레이터에 대해 자세히 설명한다. 그리고 IV 장에서는 대표적인 네 가지 공격과 가상화 모듈 내 적용에 대해 다루며, 마지막 장에서는 결론과 향후 연구를 설명한다.

Ⅱ. 관련 연구

국내의 사이버 보안 훈련은 주로 Jeopardy 형식에 기반을 둔 반면, 국외의 사이버 보안 훈련은 주로 실시간 형태의 사이버 보안 훈련에 집중되어 있다[5]. 대다수의 교육 프로그램 활동이 학습형에서 체험형으로 넘어온 단계이기도 하나, 훈련과 작전을 세울 수 있는 전략형 가상화 기반 사이버훈련 시뮬레이션으로 발전해 나갈 수 있는 연구와 기술 확보가 필요하다. 더욱이 자동차 보안 영역에서도 효과적이고 안전한 사이버전 훈련을 제공하기 위해 사이버훈련 가상화 개발환경의 구축은 필수적이라 할 수 있다.

국내에서는 사이버 위기 경보에 대응하기 위한 사이버 방어 훈련장을 제안한 연구가 진행되었다[6]. 사이버 훈련장은 네 가지의 참가자 수행역할과 영역을 설정하고, 이에 따른 구체적인 설계 방법을 제안한다. 설계된 훈련장을 바탕으로 다양한 사이버훈련 시나리오를 구성하고, 각 시나리오에 따라 공격 및 방어 훈련을 수행할 수 있다. 국외에서는 데이터셋 생성, 가상화 개발환경, 에뮬레이터 구성 등 다양한 연구가 진행되고 있다. 데이터셋 생성의 경우 실제 사용자의 웹사이

트 사용 데이터를 기반으로 행동 시퀀스를 생성하는 연구가 있다[7]. 이외에 사이버안보훈련 시스템에서 MITRE ATT&CK 프레임워크를 기반으로 사이버 위협을 모델링하는 도구 및 플랫폼 또한 연구되고 있다 [8,9].

Ⅲ. 가상화 개발환경 구성

3.1. 가상의 CAN 네트워크 인터페이스 자동활성화

차량 내부 네트워크 시뮬레이터가 작동하기 전에 먼저 가상의 CAN 네트워크 인터페이스가 자동으로 활성화되도록 하는 구성이 필요하다. 본 논문에서의 가상의 CAN 네트워크 인터페이스는 가상머신에서 간단한 부트스트랩 (bootstrap) 명령어 실행을 통해 시작되며, 파이썬 패키지와 Ubuntu 서비스목록의 설치 명령이 자동 실행됨으로써 설치가 완료된다. 가상의 CAN 네트워크 인터페이스는 Ubuntu 18.04, 20.04, 22.04 등에서 구성할 수 있으며, Microsoft Azure, Amazon Web Services, Google Cloud Platform 등 다양한 가상머신 환경에서도 호환이 가능하다. 또한, Docker Hub를 통해 배포되는 공식 Ubuntu 이미지에서도 구동이 가능하다. 본 논문에서 쓰인 패키지와 서비스 목록은 아래의 [표 1]과 같다.

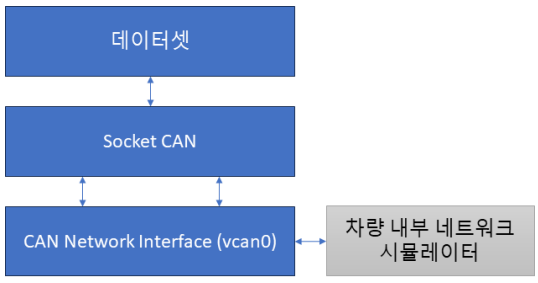
〔표 1〕 사이버훈련 프레임워크에 사용된 패키지/서비스

분류	패키지/서비스
Ubuntu APT	can-utils, nvim
Ubuntu System	jupyter.service, can-replater.service
Miniforge	Python 3.11, Numpy, scipy, matplotlib, ipython, scikit-learn, pandas, pillow, jupyter, python-can, cantools

3.2. 내부 네트워크 시뮬레이터

가상의 CAN 네트워크 인터페이스가 자동으로 활성화가 되면, 내부 네트워크 시뮬레이터와 공격모듈과 관련된 UI가 자동으로 Ubuntu Systemd에 의해 백그라운드에서 실행되어 시작과 동시에 준비 상태를 유지하게 된다. 내부 네트워크 시뮬레이터는 수집한 CAN 프로토콜 형식의 데이터셋을 Linux의 SocketCAN 모듈을 통해 가상머신 내부로 읽어와 커널 수준에서 CAN 통신을 처리한다. 또한, SocketCAN은 Linux 커널의 네트워킹 서브 시스템에서 CAN 통신을 위한 네트워킹 스택과 드라이버를 제공하므로, 내부 네트워크 시뮬레이터는 읽어온 데이터셋을 내부에서 재생하여, 지속적으로 CAN 패킷을 생성하고 가상의 내부 네트워크에 전송한다. 이러한 과정은 실제 주행 중인 네트워크 상황을 모방하게 되는 것으로써, 데이터셋의 모든 내용이 재생되면 처음부터 재생하는 사이클로 동작한다. [그림 2]는 내부 네트워크 시뮬레이터의 동작 방식을 그림으로 나타낸 것이다.

내부 네트워크 시뮬레이터 작동 시 본 시스템을 점검하거나 CAN 패킷을 모니터링 하기위해 여러가지 명령어를 사용할 수 있다. 먼저, candump vcan0 명령어는 간단하고 빠르게 CAN 메시지를 모니터링하고 출력하는 역할을 한다. 이와 유사하게, cansniffer vcan0 명령어는 CAN 메시지 모니터링과 함께 검색 및 필터링 등의 기능을 제공한다. 다음으로, ifconfig vcan0 명령어는 vcan0 인터페이스 상태를 확인하며 Rx, Tx 카운트/바이트를 관찰하여 통신 상태를 파악한다. 시뮬레이션 측면에서, service can-replayer status 명령어는 내부 네트워크 시뮬레이터의 상태를 확인하는 데 사용된다. 시뮬레이터가 동작 중인지 확인하여 신뢰성을 보장한다. 또한, 시뮬레이터를 재시작하는 명령어인 service can-replayer restart를 소개하며, 이를 통해 시뮬레이션 환경의 안정성을 유지한다. 마지막으로, 논문은 가상화 환경의 상태를 확인하는 데에 service jupyter status와 netstat -antp | grep LISTEN 명령어를 이용한다. 이를 통해 가상화 환경의 동작 상태를 파악하고, 특정 포트를 리스닝하는 프로세스를 확인하여 시스템 상태를 점검한다. 가상화 환경을 재시작하기 위해 service jupyter restart 명령어를 소개하



〔그림 2〕 내부 네트워크 시뮬레이터 통신 방식

며, 문제가 발생할 경우 프로그램을 재시작하여 정상 동작을 유지하는 방법을 제시한다. 이러한 명령어들은 효과적인 내부 네트워크 시뮬레이션, 가상화 환경 관리를 지원함으로써 차량용 사이버훈련 프레임워크의 안정성과 성능 향상에 기여한다.

3.3. 데이터 셋

3.3 장에서는 내부 네트워크 시뮬레이터에서 사용하는 데이터셋에 대해 다룬다. 가상화기반 사이버훈련 프레임워크 설계를 위해 수집된 데이터셋은 2017년식 현대자동차 LF 쏘나타 1.7 eVGT 차량을 대상으로 한다. 해당 데이터셋은 Kvaser Memorator Professional HS/HS CAN 인터페이스라는 도구를 사용하여 약 23분 26초 동안 시내 주행 중에 발생한 데이터를 수집한 것이다. [표 2]는 LF 쏘나타로부터 데이터 수집할 시 차량의 상태를 상세하게 기록한 내용이다.

해당 데이터셋은 총 3,066,366개의 CAN 패킷으로 구성되며, 초당 약 2,181개의 메시지가 발생한다. 총 62개의 Arbitration ID로 이루어져 있는 데이터셋의 압축 전의 용량은 282.1MB이고, tgz 확장자로 압축한 후의 용량은 약 56.9MB이다. 데이터는 Timestamp (microsecond 단위), Bus ID (1로 통일), Arbitration ID, 송수신 여부 (수신을 의미하는 Rx로 통일), DLC (Data Length Code, 페이로드 길이), Payload, 메시지 카운터로 구성되어 있어 학습자가 쉽게 열람할 수 있도록 텍스트 파일로 추출되어 있다.

대부분의 차량 제조사들은 차량 내부 네트워크 트래픽 분석을 위한 CAN database를 제공하지 않는다. 그렇다 보니, 역공학을 통해 일부 트래픽의 의미를 부분적으로 식별할 수 있을 뿐, 모든 정보를 파악하는 데에는 한계가 존재한다. 우선, 본 논문에서는 OpenDBC 프로젝트에 공개된 현대자동차 LF 쏘나타와 관련된 CAN database를 통해 수집된 데이터셋 내 각 Arbitration ID 특징을 분석하고 요약하였다. 수집한 데이터셋 중에서 Arbitration ID의 기능을 분석하지 못한 6종류를 제외하고는 총 50종류의 Arbitration ID를 분석할 수 있었다. 각 Arbitration ID의 기능을 상세하게 분석하는 것은 가상화기반 사이버훈련 프레임워크 개발환경 중 공격 모듈 구성 시 Impersonation attack를 위해 사용된다. 분석된 대부분의 Arbitration ID는 Transmission Control Unit (TCU), Engine Management System (EMS), Motor-Driven Power Steering System (MDPS), Electronic Parking Brake (EPB) 등과 관련된 주요 파워트레인의 데이터를 담고 있다, 즉, 실제로 분석된 CAN ID를 통해 공격을 수행했을 시, 차량의 안전 측면에 있어 공격의 파급력이 크다고 볼 수 있다. OpenDBC 프로젝트에서 획득한 CAN database의 정확도를 보장하기 위해 아래와 같이 주요 데이터를 시각화하였다.

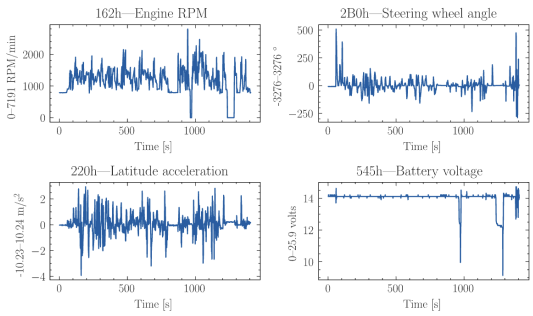
〔표 2〕 데이터셋 수집 시 차량 상태

분류	값
자동차 현재 속도 (km/h)	45km/h 이하
엔진 회전속도 (RPM)	3000 RPM 이내
운전대 각도 (degree)	우측 조향 시 양수의 각도 좌측 조향 시 음수의 각도
엔진 온도 (섭씨)	섭씨 약 85~95도
종가속도 (m/s^2)	감속 시 최대 -4m/s^2 가속 시 0~2m/s^2
배터리 전압 (Volt)	약 14V
엔진 토크 증가 요청 (%)	변속 및 가속 시 값 상승
흡기 공기 온도 (섭씨)	섭씨 약 27~40도

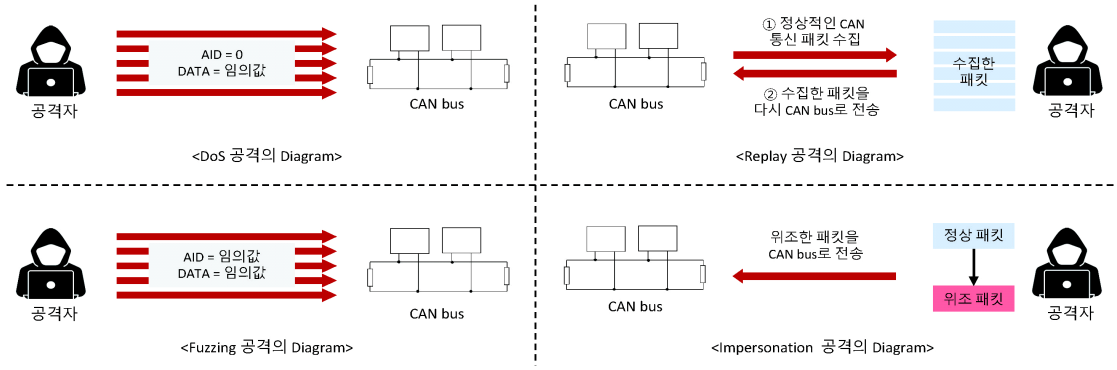
Ⅳ. In-vehicle 공격 벡터별/유형별 환경 설계

4.1. 공격 유형

본 장에서는 가상화 기반 사이버훈련 프레임워크 중 공격 모듈을 구현하기 위해 DoS (Denial of Service) attack, Fuzzing attack, Replay attack, Impersonation attack까지 총 네 가지의 공격 방식을 설명한다.



〔그림 3〕 주요 센서 데이터 시각화



〔그림 4〕 네 가지 공격 유형 (DoS attack, Fuzzing attack, Replay attack, Impersonation attack)

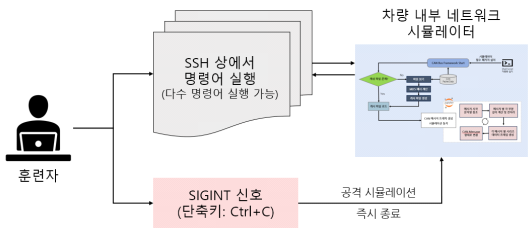
첫 번째로 DoS attack은 CAN 메시지 콘텐츠 (Arbitration ID, Payload) 중 Arbitration ID는 메시지 식별자로서 ID의 값이 낮을수록 우선순위가 높다는 점을 이용한다. CAN bus 내에 특정 데이터를 계속해서 전송함으로써 정상 메시지의 전송을 지연/방해하는 공격이다[10]. 두 번째로, Fuzzing attack은 CAN 기반 차량 내부 네트워크 트래픽에 인증/암호화 기법이 없다는 점을 이용한 공격이다. 해당 공격은 Arbitration ID와 Payload 모두에 임의 값을 넣어 구성한다. 이러한 무작위 메시지를 전송하여 이상 동작을 유도하도록 설계하였다. Replay Attack은 CAN bus에서 수신된 CAN 패킷 메시지를 일정 시간 동안 모아 다시 전송하면서 수행되는 공격이다[11]. 마지막으로, Impersonation attack은 차량 내부 네트워크에서 사용하는 특정 Arbitration ID와 Payload를 정상 데이터인 것처럼 위조한다. 이를 통해 특정 동작을 유도하여 공격할 수 있도록 설계하였다[12]. [그림 4]는 네 가지 공격 유형을 보여준다. 네 가지 공격 유형을 차량용 사이버 훈련 프레임워크 내 공격 모듈에 적용한다는 것은 실제 차량에서도 발생할 수 있는 차량의 이상 상태로 출력하여 사이버훈련 프레임워크 사용자들의 훈련 집중도와 훈련 이해력을 도모하기 위함이다.

4.2. 공격 모듈 구성

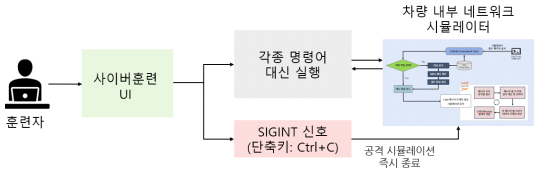
4.1장에서 소개된 네 가지 공격 유형은 공격 모듈 내에서 사용자의 선택을 통해 수행된다. 공격 모듈은 설정 방식에 따라 직접 실행과 간접 실행의 두 가지 실행 방법으로 나누어 적용될 수 있다.

먼저, 직접 실행은 사용자가 CLI에서 직접 명령어를 실행하는 경우를 의미한다. 사이버훈련 프레임워크에 대해 이해도가 높은 고급 훈련자를 대상으로 하고 있으며, SSH 상에서 명령어를 자유롭게 수행할 수 있는 경우 해당이 된다. 특히, 직접 실행의 경우, 각 공격 명령을 두 개 이상 동시에 실행하여 복합적인 공격 상황을 시뮬레이션할 수 있다. 또한, 키보드를 통해 SIGINT 명령어를 발생시켜 공격 시뮬레이션을 즉시 종료시킬 수 있다. [그림 5]는 직접 실행되는 공격 모듈을 도식화한 것이다.

다음으로, 간접 실행은 훈련자가 사이버훈련 UI 상에서 공격 유형, Arbitration ID 등의 파라미터를 지정한 뒤 시작 버튼을 통해 공격 프로그램을 실행하는 경우를 의미한다. 사이버훈련을 받는 일반 교육자를 대상으로 하며, 사이버훈련 UI가 훈련자를 대신하여 공격 명령어를 대신 실행해준다. 공격 시뮬레이션을 중단하고 싶은 경우 사이버훈련 UI 상에서 '중단' 버튼을 누름으로써 공격 프로그램을 종료할 수 있다. [그림 6]은 간접 실행되는 공격 모듈을 도식화한 것이다.



〔그림 5〕 직접 실행되는 공격 모듈



〔그림 6〕 간접 실행되는 공격 모듈

Ⅴ. 결론 및 향후 연구

대다수의 교육 프로그램 활동이 학습형에서 체험형으로 넘어온 단계이나 훈련과 작전을 세울 수 있는 전략형 가상화 기반 사이버훈련 시뮬레이션으로 발전해 나갈 수 있는 연구와 기술 확보의 확보가 필요하고, 더욱이 차량 내부 네트워크를 대상으로 하는 가상화 기반 사이버훈련 프레임워크 설계 제안이 필요하다. 본 논문에서는 차량 사이버훈련 프레임워크를 제안하기 위해 가상화 개발환경, 내부 네트워크 시뮬레이터, CAN 프로토콜을 대상으로하는 대표적인 공격 기술 등을 설명하였다. 이러한 가상화 기반의 차량용 사이버훈련 프레임워크는 자율주행 차량 사고의 위험이나 다른 특수한 제약 없이 사용자의 학습 경험을 확장 시킬 수 있다. 기존의 가상화 기반 사이버훈련 교육 콘텐츠와는 달리 일반 사용자들이 접근하기 보다 쉬운 형태로 개발이 가능하다. 향후 연구로는 제시된 공격 시나리오를 탐지할 수 있는 탐지 모듈과 사이버훈련 학습 결과를 출력할 수 있는 모듈 제작을 수행하고자 한다.

참 고 문 헌

[1] 한국인터넷진흥원(KISA), Security-Gym, June 2022, https://www.kisa.or.kr/

[2] 사이버안전훈련센터, June 2022, https://www.cstec.kr/ cstec/kor/html/sub01/sub0101.html

[3] CyberGym, Israel, June 2022, https://www.cybergym. com/#section_1

[4] Raytheon Technologies, USA, June 2022, https://www.raytheon.com/cyber/ capabilities/range

[5] 이대성, “국내외 사이버 보안 훈련 동향”, *한국정보통신학회논문지*, 25 (6), pp.857-860, 2021

[6] 최영한, 장인숙, 황인택, 김태균, 홍순좌, 박인성, 양진석, 권영재, 강정민, “사이버위기 경보 기반 사이버 방어 훈련장 설계 및 구축 연구”, *정보보호학회논문지*, 30 (5), pp.805-821, 2020.

[7] Oesch, T Sean, Bridges, Robert, Verma, Miki, Weber, Brian, & Diallo, Oumar, “D2U: Data Driven User Emulation for the Enhancement of Cyber Testing, Training, and Data Set Generation”, *14th Cyber Security Experimentation and Test Workshop*, 2021.

[8] S. Maxwell, M. Lucas, D. Bowman, T. Richer, J. Kim, D. Marriott, “CybORG: A Gym for the Development of Autonomous Cyber Agents”, *International Joint Conference on Artificial Intelligence,* 2021.

[9] 김동화, 김용현, 안명길, 이희조, “사이버 보안 훈련을 위한 ATT&CK 기반 사이버 위협 모의 기술 연구”, *한국컴퓨터정보학회논문지*, 25 (9), 71-80, 2020.

[10] Han, Mee Lan, Byung Il Kwak, and Huy Kang Kim. "Anomaly intrusion detection method for vehicular networks based on survival analysis." Vehicular communications 14 (2018): 52-63.

[11] Han, Mee Lan, Byung Il Kwak, and Huy Kang Kim. "Event-triggered interval-based anomaly detection and attack identification methods for an in-vehicle network." IEEE Transactions on Information Forensics and Security 16 (2021): 2941-2956.

[12] Lin, Yubin, et al. "An evolutionary deep learning anomaly detection framework for in-vehicle networks-CAN bus." IEEE Transactions on Industry Applications (2020).

〈저 자 소 개〉

조 영 복 (YoungBok Jo)
학생회원
2018년 3월~현재 : 고려대학교 세종캠퍼스 인공지능사이버 보안학과 학사과정
<관심분야> 침해사고 대응, AI 보안, 사이버 보안

최 수 빈 (Subin Choi)

2019년 3월~현재 : 고려대학교 세종캠퍼스 인공지능사이버 보안학과 학사과정

<관심분야> 취약점 분석, 자동차 보안, 사이버 보안

오 병 윤 (OH ByeongYun)

2018년 3월~현재 : 고려대학교 세종캠퍼스 인공지능사이버 보안학과 학사과정

<관심분야> IoT 보안, 자동차 보안, 사이버 보안

최 영 호 (YongHo Choi)

2019년 3월~현재 : 고려대학교 세종캠퍼스 인공지능사이버 보안학과 학사과정

<관심분야> 자동차 보안, 시스템 보안, 정보보호

김 호 준 (Hojun Kim)

2019년 3월~현재 : 고려대학교 세종캠퍼스 인공지능사이버 보안학과 학사과정

<관심분야> 자동차 보안, 시스템 보안, 정보보호

정 성 훈 (Seonghoon Jeong)

2015년 2월 : 충북대학교 정보통신공학부 학사 졸업

2017년 2월 : 고려대학교 정보보호대학원 석사 졸업

2023년 2월 : 고려대학교 정보보호대학원 박사 졸업

2023년 3월~현재 : 고려대학교 정보보호연구원 박사후연구원

<관심분야> 데이터중심보안, 차량용 침입방지시스템

곽 병 일 (Byung Il Kwak)

종신회원

2013년 2월 : 세종대학교 컴퓨터공학과 학사 졸업

2021년 2월 : 고려대학교 정보보호대학원 정보보호학과 박사 졸업

2021년 8월 : 고려대학교 정보보호대학원 연구교수

2021년 9월~현재 : 한림대학교 정보과학대학 소프트웨어학부 조교수

<관심분야> 네트워크 보안, IoT 보안, 자동차 보안, 침입 탐지, 이상 탐지

한 미 란 (Mee Lan Han)

종신회원

2002년 2월 : 동덕여자대학교 컴퓨터과학과 졸업

2015년 8월 : 고려대학교 정보보호대학원 석사 졸업

2020년 8월 : 고려대학교 정보보호대학원 박사 졸업

2020년 9월~2021년 8월 : 고려대학교 정보보호연구원 연구교수

2021년 9월~2022년 8월 : 고려대학교 인공지능사이버보안학과 산학협력중점교수

2022년 9월~현재 : 고려대학교 인공지능사이버보안학과 조교수

<관심분야> 사이버 범죄자 행위분석, 이상징후탐지 및 식별, 임베디드 보안