정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

차량 네트워크 공격 대응을 위한 가상화 사이버 훈련 개발환경 사례 연구

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

요 약

차량 기술의 발전으로 커넥티드 및 자율주행 차량 환경과 같은 차량 기술의 발전은 운전자에게 편의와 안전을 위한 기능을 제공한다. 하지만 이러한 장점들에도 불구하고 사이버 공격의 다양한 취약점 노출되어 있다. 최근까지 자동차 내부 네트워크로써 가장 널리 사용되는 통신기술인 CAN(Controller Area Networks) 통신은 대부분 차량의 동력을 담당하는 역할을 하다보니, 보안 문제의 중심에 서게 될 수 있다. 다양한 이기종 네트워크에서 구성된 가상화 기반의 사이버 훈련 프레임워크에 대해 설명하고자 한다. 이러한 사례 연구는 차량에 대해 물리적인 실험 환경에서의 모의침투와 같은 테스트가 어렵고, 보안과 안전이 함께 고려되어야 하는 특수성을 가진 차량 내부 네트워크의 사이버 훈련 프레임워크 설계에 도움을 줄 것이다. 본 논문에서는 가상화 개발환경 구축 사례 조사, 가상화 개발환경 구현과 차량의 공격 시나리오 및 탐지 프레임워크의 동향을 설명한다.

Ⅰ. 서 론

현대 사회에서는 인터넷 기술의 지속적인 발전으로 인해 사이버 공격과 보안 위협이 증가하고 있다. 이에 따라 기업들은 고객 정보와 핵심 기업 정보의 유출 위험에 직면하고 있으며, 이러한 위협에 대응하기 위해 사이버 보안 인식과 역량 강화가 매우 중요시되고 있다. 또한, 사이버 보안에 대한 필요성이 초등 및 중학교 교육과정에서도 강조되며, 사이버 교육용 콘텐츠에 대한 수요가 점점 증가하고 있다.

특히 자율주행차와 임베디드 시스템의 보안 문제는 점점 중요해지고 있다. 자율주행차는 기계와 전자기기의 상호작용이 매우 복잡하므로, 가상화 기반 사이버 훈련 도메인에서는 이기종 네트워크와 고도의 보안체계를 고려한 특별한 사이버 훈련 환경이 필요하다. 사이버 훈련 프레임워크는 자율주행차 보안전문가를 양성하고, 실제 물리적 실험 환경에서의 높은 비용과 안전 위험을 최소화할 수 있다. 따라서, 본 논문에서는 다양한 가상화 개발환경 구축 사례, 가상화 개발환경 구현과 차량의 공격 시나리오 및 탐지 프레임워크의 동향을 살펴보고자 한다.

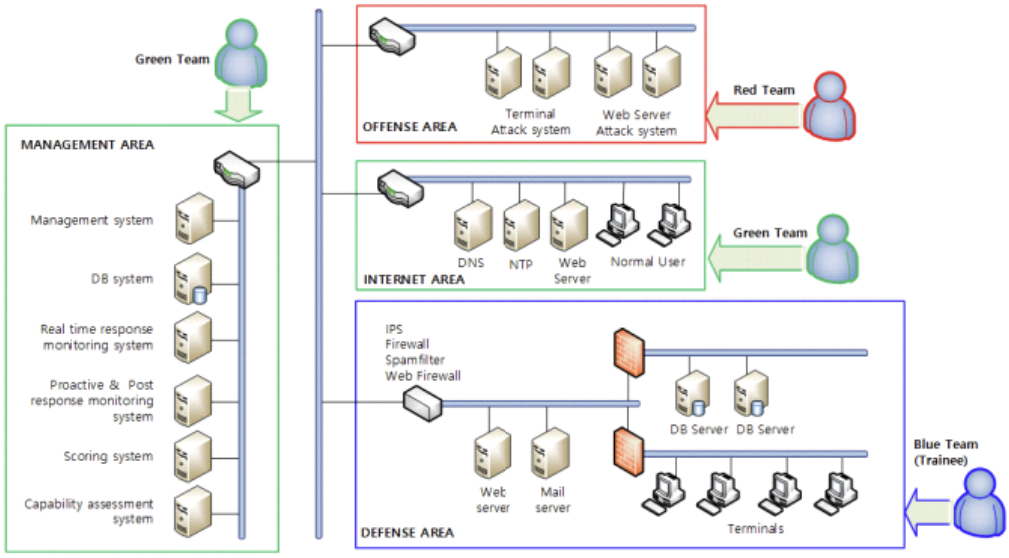
Ⅱ. 가상화 개발환경 구축 사례

2.1. 국내/외 사이버 보안 훈련 동향

국내의 사이버 보안 훈련은 주로 Jeopardy 형식에 집중되어 있다. Jeopardy 형식의 대회는 웹, 포렌식, 암호학, 시스템 등의 문제들을 주어진 시간 안에 푸는 대회이며, 참여자는 해결된 모든 과제에 대해 점수를 얻을 수 있으며, 문제의 취약점을 통해 공격 성공 후 점수를 얻을 수 있는 ‘flag’를 얻는다. 국외의 경우, 주로 실시간 형태의 attack-defense 형식의 사이버 보안 훈련이 주로 진행된다. 보통 참여자 팀에게 취약한 서비스를 가진 자체 네트워크(또는 하나의 호스트)를 지급하고, 자신의 서비스는 패치하여 방어하는 반면 상

“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 인공지능사이버 보안학과 (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〕 사이버 방어 훈련을 위한 사이버 훈련장 범위

대 팀의 서비스는 공격하는 방식의 훈련이다. 방어와 공격을 둘 다 진행하고, 실시간으로 진행된다는 점에서 Jeopardy 형식의 훈련과는 차이를 보인다.

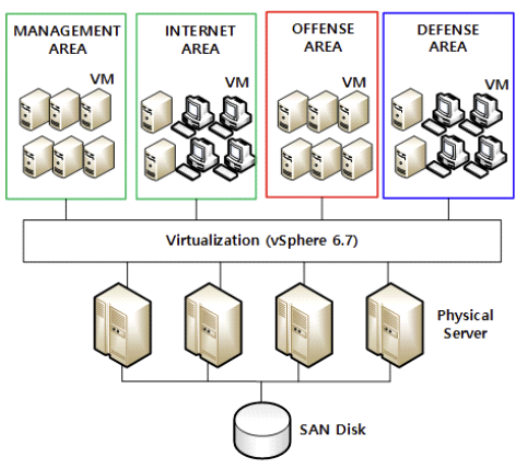
2.2. 사이버 훈련장 구축 사례

2.2.1. 사이버 위기 경보 기반 사이버 방어훈련장

사이버 위협에 대한 가상 기반의 사이버 훈련장의 경우, 몇 가지 유형으로 설명할 수 있다. 첫 번째 유형이 사이버 위기 경보를 기반으로하는 사이버 방어 훈련장이다. 사이버 위기 경보에 기반한 사이버 방어 훈련장은 실시간 방어 수행이 가능하도록해 사이버 회복력을 강화하도록 제안되었다. 또한, 피해 시스템에 대한 사고 조사를 수행하는 사후대응 훈련을 지원하는 환경을 제공한다. 사이버 위기 경보 수준에 따라 주의, 경계, 심각한 경보가 발령될 때, 해당 경보에 따라 예방 보안을 확인할 수 있다. 사이버 훈련장 환경은 공간과 비용 문제로 인해 점점 물리 시스템보다 가상화 기술을 이용하여 설계되고 구현되고 있으며, Cyber-Physical System(CPS)의 경우는 사이버 공간과 접속하는 물리 시스템이 필요하므로 물리 시스템을 병행하여 운영하게 된다 [1].

사이버 훈련 시나리오는 사이버 훈련장 환경 위에 사이버 공격이나 방어를 수행할 수 있는 훈련 내용을 주입해서 만든다. 시나리오는 문제 풀이 형식이나 실전을 위한 이야기 흐름이 될 수 있으며, 주어진 임무를 수행함으로써 사이버 보안에 대한 역량을 강화할 수 있다.

훈련 운영은 훈련 참가자의 수행 역할에 따라 각각 Red Team, Blue Team, Green Team, 그리고 White Team의 4가지로 나눈다. Red Team(RT)은 사이버 공격을 수행한다. 사이버 공격을 하는 시나리오의 경우는 RT가 훈련생이 된다 [3]. 사이버 방어 훈련장에서 Blue Team(BT)은 실시간으로 진행되는 사이버 공격



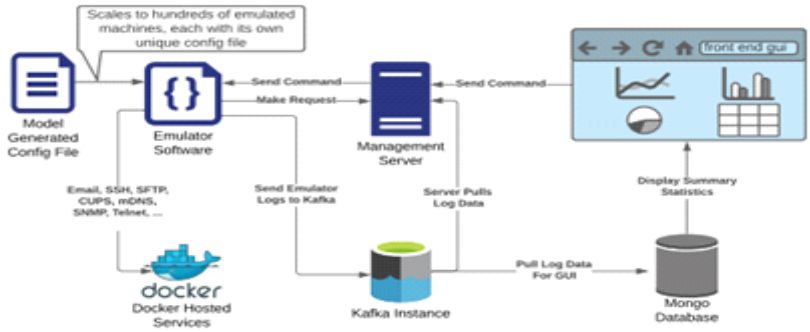
〔그림 2〕 사이버 방어 훈련장 구축 방법론

에 대한 방어를 수행하여 훈련생은 사이버 위협에 대응하는 역량을 향상할 수 있다. Green Team(GT)은 훈련 대상이 되는 사이버 훈련장 환경을 구축하여 직접적으로 훈련에 참여하지는 않지만, 시나리오가 주입되는 훈련 A 환경을 구축한다[4]. White Team(WT)은 훈련 시나리오를 사이버 훈련장에 적용하고 사이버 훈련을 운영하며, 점수를 스코어링 한다[5].

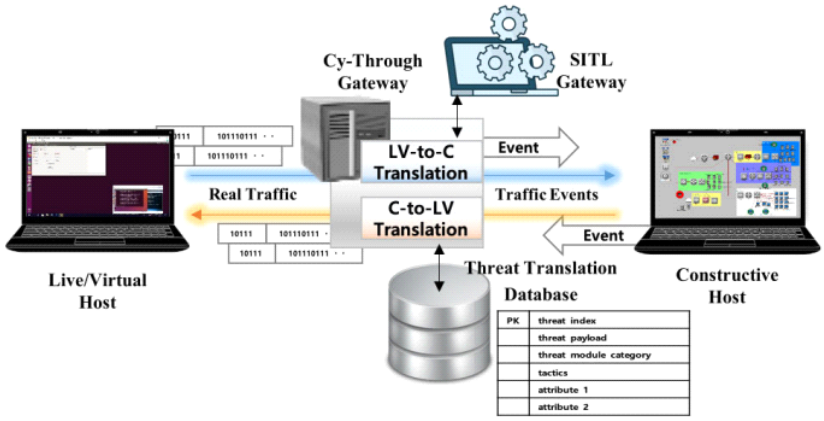
사이버 훈련장은 관리 영역, 인터넷 영역, 공격 영역, 방어 영역으로 나누어진 훈련 환경을 제공한다. 관리 영역은 Green Team에서 담당한다. 관리영역에서는 관리시스템, DB 시스템, 실시간 대응 모니터링 시스템, 예방보안과 사후 대응 모니터링 시스템, 훈련 점수 시스템, 역량평가 시스템을 구축 및 관리한다. 인터넷 영역은 방어영역 내 시스템이 정상 인터넷 활동을 할 수 있도록 인터넷의 웹사이트와 사용자를 모사한다. 이것은 방어영역으로 정상 트래픽을 발생시켜 실제 사이버 사고 분석 환경을 제공하며, 실제 정상적인 환경과 유사하게 구축하기 위해서 정상 웹사이트 모사 시스템과 정상 사용자 모사 시스템이 필요로 한다. 공격영역은 Red Team에서 담당한다. 실시간 대응 훈련 시 방어영역 내에 있는 웹서버와 단말을 공격하며 사이버 위기 경보의 단계에 따라 공격의 수위가 달라진다. 공격영역은 웹서버 공격 시스템과 단말 공격 시스템으로 이루어진다. 방어영역은 Blue Team에서 담당하고, 방어영역은 Blue Team에서 담당한다. 방어영역은 훈련생들이 사이버 공격으로부터 보호를 해야 하는 영역이며, 시스템 구성은 훈련 시나리오에 따라 다양하다. 기본적으로 정보보호 시스템, 웹서버, DB 서버와 단말로 구성된다. 예방 보안, 실시간 대응, 사후대응 훈련 시나리오별로 사이버 위협에 취약한 단말 및 서버가 설치된다[2].

2.2.2. D2U 기반 사이버 방어훈련장

D2U 방식의 사이버 훈련장은 사이버 검증, 훈련, 그리고 데이터셋 생성에 사용할 수 있는 어플리케이션 트래픽 시퀀스를 이용한다 [6]. D2U는 실제 사용자 데이터를 기반으로하는 생성 모델을 사용하여 테스트 및 교육에 사용할 수 있는 무제한의 새로운 사용자 행동 시퀀스를 제공한다. D2U 구조는 확장성이 뛰어나 수백 또는 수천 개의 에뮬레이터를 동시에 실행할 수 있으며, 확장 가능하여 Python을 사용하여 최소한의 노력으로 추가 사용자 작업을 추가하고 확장할 수 있다. 모델이 생성한 고유한 구성 파일은 각 장치에서 실행되는 에뮬레이터 소프트웨어에 제공한다. 생성된 구성 파일과 수집된 데이터를 기반으로 구축된 모델을 사용하며 에뮬레이터 소프트웨어는 웹 검색, 문서 작성 및 편집, 이메일, ssh, ftp, shell 명령 및 기타 일반적인 동작을 포함하여 지정된 작업을 수행한다. 실행 중인 에뮬레이터 소프트웨어는 Kafka 스트림을 사용하여 작업 및 상태를 수행한다. 환경에는 MEAN(MongoDB, Express.js, AngularJS, Node.js) 스택을 사용하여 구축된 웹사이트와 함께 실행되는 관리 서버가 있으며, 에뮬레이터에 대한 요약 통계와 현재 작업, 해당 에뮬레이터에 대해 받은 마지막 하트비트 메시지 시간 및 기타 관련 정보가 표시된다. 이 웹사이트는 또한, 서버를 통해 개별 에뮬레이터에게 메시지를 보내는 데 사용될 수 있으며, 서버는 에뮬레이터 역할은 한다. 이러한 메시지는 인터럽트로 전송되어 에뮬레이터가 지정된 작업을 수행하기 위한 현재 작업을 중지하거나 기존 작업 대기열의 끝에 추가된다.



〔그림 3〕 D2U 기반의 사이버 훈련장 구조



〔그림 4〕 Cy-Through Gateway 모드 작동 순서도

Ⅲ. 가상화 개발환경

3.1. 사이버 위협 대상

사이버 위협 대상은 크게 5가지로 구분할 수 있다. 인프라 및 네트워크 장비, 서버, 웹 응용 프로그램, 엔드 포인트 디바이스 이용자, IoT 및 스마트기기가 포함된다. 첫 번째로, 공격자들은 라우터, 스위치, 방화벽 등의 네트워크 장비에서 트래픽을 가로채거나 익명으로 시스템에 침입할 수 있다. 이에 따라 기업의 기밀 정보나 개인 정보가 노출되거나, 시스템에 추가적인 피해를 준다. 두 번째로, 웹 서버, 파일 서버, 데이터베이스 서버 등 중요한 서버들이 공격 대상이다. 공격자들은 서버의 취약점을 찾아 시스템을 침입하거나, 서비스를 중단시키려고 시도한다. 세 번째로, 웹 기반의 응용 프로그램을 공격자들이 주요 대상으로 삼는다. 회원 가입 및 로그인, 게시판 등 적절한 보안 조치를 갖추지 못한 경우, 공격자들은 사이트의 취약점을 통해 피해를 주거나, 데이터를 탈취할 수 있다. 네 번째로 개인이 사용하는 PC, 태블릿, 스마트폰 등의 엔드 포인트 디바이스로 공격 대상이 될 수 있다. 악성 소프트웨어나 피싱 공격 등을 이용해 개인 정보를 탈취하거나, 디바이스를 악용해 추가적인 공격을 수행할 수 있다. 마지막으로, 가정 및 기업에서 사용되는 IoT, 스마트 기기이다. 가정 및 기업에서 점차 사용자가 늘어나면서 공격 대상이 되고 있다. 기기에서 발생하는 보안 취약점을 이용해 공격자들은 원격으로 기기에 침입하거나, 사생활에 침범하는 행위를 시도한다.

3.2. 가상화 개발환경 사용도구

CybORG는 시뮬레이션 및 에뮬레이션 모드를 통합한 연구 도구이다. CybORG는 규모 강화학습을 지원하기 위한 목적으로 개발되었다 [8]. CyTEA는 사이버 안보훈련 시스템에서 사용되는 도구이다 [7]. CyTEA는 MITRE ATT&CK 프레임워크를 기반으로 모의 사이버 위협을 모델링하는데 사용한다. 이 도구는 모의 훈련 과정에서실제 사이버 위협에 가까운 환경을 구현하고 유사성을 평가하여 효과적인 보안 대책이 개선하는데 도움이 된다는 것을 주장한다. MITRE ATT&CK 프레임워크는 사이버 보안 훈련 시스템에서 사이버 위협을 모델링하고, 모의 사이버 위협을 생성하는 역할을 한다. 공격자가 실제로 사용하는 전략과 기술을 정의하고, 이를 기준으로 공격자와 유사한 위협의 조합을 만들어낸다.

3.3. 에뮬레이터 & 시뮬레이터 구성

3.3.1. Cy-Through

사이버 위협에 대응하기 위해 다양한 충실도 수준의 시나리오 시뮬레이션 모델을 지원하고 Live, Virtual, Constructive(LVC)를 합쳐 상호운용이 가능한 Cy-Through 사이버 보안 시뮬레이션 플랫폼을 제안한다 [9]. Cy-Through는 게이트웨이와 에이전트로 구성된다. 게이트는 위협 관련 패킷의 교환을 쉽게 하여 Live, Virtual, Constructive 간의 변환을 지원한다. 사이버 공격 시나리오에서 시뮬레이션하고 영향을 분

석하여 여러 환경 속에서도 위협에 효과적으로 대응할 수 있도록 설계되었다. Cy-Through Gateway는 Cy-Through 플랫폼의 기능 중 하나로 위협 관련 패킷을 관리하는 데 사용된다. 또한, Cy-Through Gateway에서는 위협 변환 기능이 있다. 패킷에서 위협 시그니쳐를 감지할 때, 원래 페이로드를 대처하기 위해서 사전에 준비된 데이터로 교체한다.

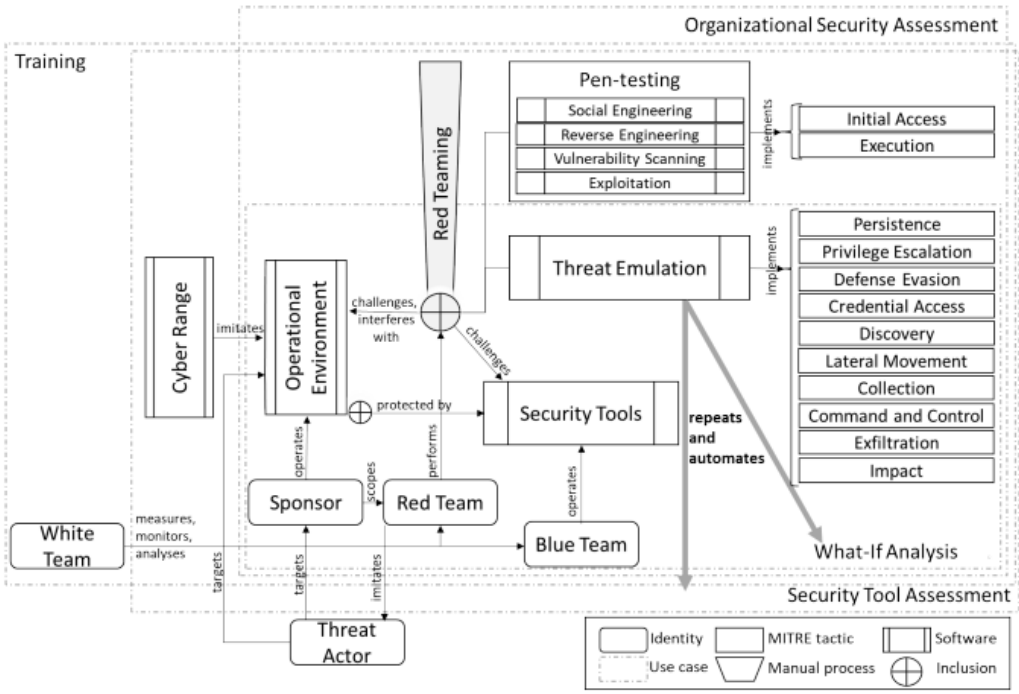
3.3.2. 오픈소스 위협 에뮬레이터

오픈소스 위협 에뮬레이터는 사이버 공격이나 악의적인 동작을 모방하는 도구이다. MITRE ATT&CK 매트릭스의 전술가 기술을 기준으로 위협 에뮬레이터들을 검토하고 비교한다 [10]. [그림 5]에서 말하는 위협 에뮬레이션의 생태계는 레드팀 활동의 핵심 구성요소로서, 다양한 이해관계자와 관련 소프트웨어 프로세스로 구성된다. 소프트웨어 및 도구는 조직의 운영 환경을 지원하고 보호하기 위해 사용하며, 소프트웨어 및 도구에는 보안 도구, 사이버 레인지, 그리고 위협 에뮬레이터 등이 포함된다. 위협 에뮬레이터는 교육, 보안 도구 평가, 조직 보안 평가, what-if 분석 등 네 가지 주요 사용사례에 활용한다. 이러한 위협 에뮬레이션 생태계는 레드팀 활동의 효율성과 신뢰성을 높이고 조직의 보안 수준을 향상할 수 있다.

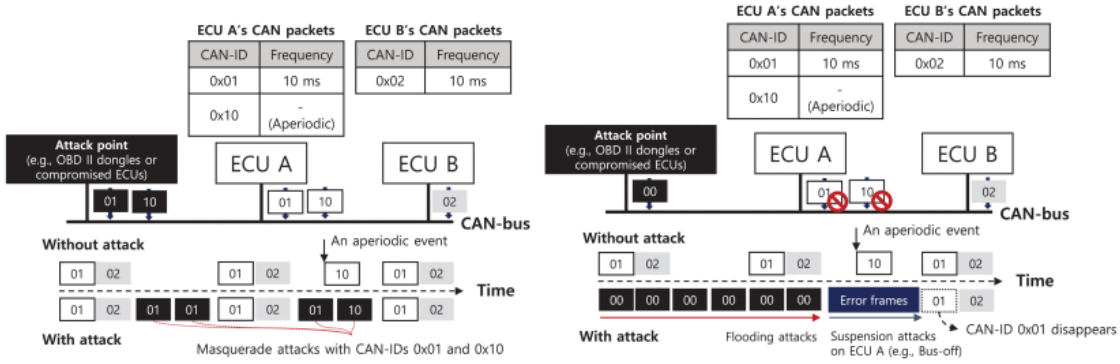
Ⅳ. 차량 In-vehicle 공격 및 탐지 유즈케이스

4.1. 차량 네트워크 공격 모델

차량 네트워크를 공격하는 방식은 매우 다양하게 존재하며, 본 절에서는 대표적인 공격 유형인 Masquerade Attack과 DoS Attack을 소개하고자 한다 [11]. [그림 5]는 Masquerade Attack과 DoS Attack을 공격자의 구체적인 공격 행위에 대한 설명과 함께 그림으로 설명한 것이다. 먼저, 차량 네트워크에서 Masquerade 공격은 공 격자가 자동차 CAN을 통해 가짜 Arbitration ID를 가지고 악의적인 명령을 전송하여 차량의 무단 통제권을 획득하는 사이버 공격의 일종이다. 이러한 유형의 공격에서 공격자는 일반적으로 message replay 또는 message fabrication을 사용하여 차량 제어를 변경한다. replay 또는 fabrication을 기반으로 하는 Masquerade 공격은 주기적 CAN 패킷 또는 비주기적 패킷을 사용한 masquerade를 통해 이루



〔그림 5〕 위협 에뮬레이터 생태계



(a) Masquerade attacks (b) DoS attacks (Flooding and suspension attacks)

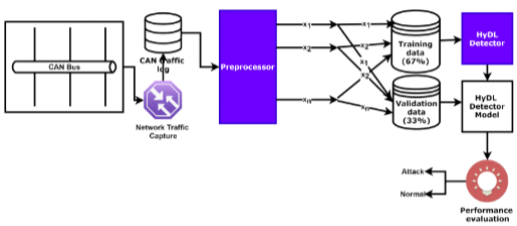
〔그림 6〕 차량용 CAN에 대한 공격 시나리오

어진다. Masquerade 공격은 적에게 차량을 무단으로 제어할 수 있으므로 매우 위험할 수 있다.

- Message replay attack: 공격자는 자동차 CAN 모니터링 중에 관찰된 CAN 패킷을 수정 없이 재생함
- Message fabrication attack: 공격자는 CAN ID 필드와 CAN 데이터 필드를 위조하여 CAN 패킷을 구성함

다음으로, 차량 네트워크에 대한 DoS (Denial of Service) 공격은 공격자가 자동차 CAN에 메시지 플러딩 공격을 하여 네트워크 대역폭을 고갈시키거나 특정 ECU에 대한 공격을 일시 중단시켜 메시지 전송을 방해하는 사이버 공격의 일종이다. DoS 공격은 Message flooding attack과 Suspension attack이 존재한다.

- Message flooding attack: 공격자는 우선순위가 높은 대량의 CAN 패킷을 지속적으로 CAN Bus에 전송하여, 우선순위가 높은 다른 CAN 패킷이 CAN 버스로 전송되는 것을 방해할 수 있음
- Suspension attack: A 혹은 B 유형의 공격자가 해당 ECU에 대해 Suspension attack을 수행하면 해당 ECU는 CAN 통신에 참여할 수 없게 됨



〔그림 7〕 HyDL-IDS Framework

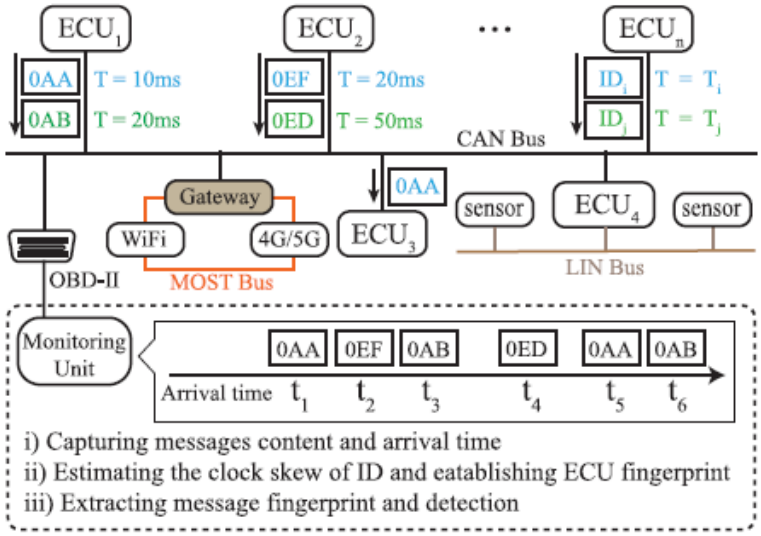
4.2. 탐지 프레임워크

4.2.1. HyDL-IDS

HyDL-IDS는 차량 내 네트워크 트래픽에서 공간적 및 시간적 특징을 추출한 후 CNN과 LSTM의 조합을 사용하여 이상 징후를 탐지하는 모델이다 [12]. DoS, Fuzzing, 분당 회전수(RPM)를 기반으로 하는 Spoofing 공격 등 네 가지 유형의 공격 데이터로 구성된 벤치마크 자동차 해킹 세트를 사용하여 HyDL-IDS를 검증하였고, 차량 내 네트워크 트래픽의 시공간 표현을 기반으로 HyDL-IDS의 성능을 나이브 베이즈, 의사 결정 트리, 다층 퍼셉트론, CNN 및 LSTM을 비롯한 다른 방법과 비교를 진행하였다. 결과적으로 제안된 HyDL-IDS를 사용하여 다양한 사이버 공격에 대해 낮은 오경보율을 보였으며 탐지 또한 약 100%에 가까운 정확도를 보여주었다. 하지만 벤치마크 자동차 해킹 데이터 세트에는 메시지 템퍼링과 같은 정교한 공격이 포함되지 않았다.

4.2.2. ClocKids IDS

ClocKids는 Clock Skew를 사용하여 spoofing, bus-off, masquerade attack과 같은 다양한 유형의 공격을 탐지하는 IDS이다 [13]. 여기서 말하는 Clock Skew란 두 클록 간의 시간 속도의 차이를 말한다. ClocKids 기존 Bus를 수정하지 않고도 컨트롤러 영역



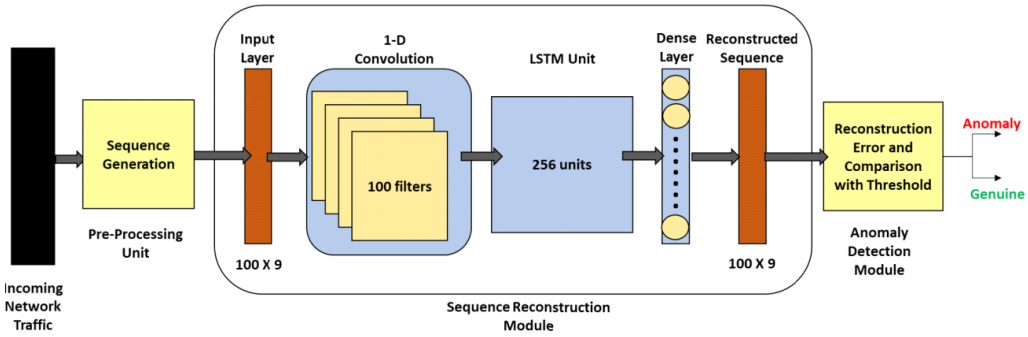
〔그림 8〕 ICV 내부 네트워크 구조와 ClocKids의 작동 원리

네트워크(CAN) 버스에 모니터링 장치로 직접 연결할 수 있다. ClocKids는 메시지 내용을 캡처하고 도착 시간을 기록하여 각 ECU의 클럭 스큐를 추정하고 지문 라이브러리를 구축하고, 지문 라이브러리를 사용하여 침입 탐지 및 공격 소스 식별을 수행한다. 새 메시지가 도착하면 ClocKids는 메시지의 지문을 추출하여 라이브러리에 있는 ECU 지문과 비교를 한다. 지문이 일치하면 메시지를 정상으로 인식하고 아닐때 침입 메시지로 인식한다.

ClocKids는 다양한 유형의 공격에 대한 탐지율이 우수하고 주기적인 분사 공격에 대한 공격의 근원을 추적할 수 있으며, 침입 메시지를 탐지할 수 있는 높은 실시간 성능을 제공했다. 또한 외부 장치로서 차량 내 인터페이스에서 직접 액세스하고 조작할 수 있으며 기존 차량 네트워크 환경을 변경하지 않고 차량 보안을 크게 향상할 수 있는 특징을 가지고 있다.

4.2.3. NovelADS

NovelADS는 최근 차량 전자 장치에서 사용되는 CAN 프로토콜의 보안 취약성을 극복하기 위해 설계된 딥러닝 기반의 침입 탐지 시스템이다 [14]. NovelADS는 딥러닝 알고리즘을 활용하며, 새로운 임곗값과 오류 재구성 접근법을 통합하여 공격을 효과적으로 탐지한다. 여러 신경망 아키텍처를 훈련하고 비교하여 가장 적합한 네트워크 구성을 선정하였다. 이를 위해 시계열 모델에서 1-D CNN 레이어를 사용하여 메시지의 공간적 특징을 학습하고, LSTM 구조를 활용하여 메시지의 시간적 흐름 특성을 추출한다. NovelADS의 탐지 시나리오는 공격자가 OBD2 포트



〔그림 9〕 제안된 방법론의 아키텍처 워크플로우

를 물리적으로 접속하거나 외부 통신 채널을 통해 원격으로 접속하여 공격을 수행할 수 있다고 가정을 한다. 학습된 NovelADS는 클라우드 서버에서 메시지를 수집하고 이상 징후 탐지 모델에 입력하여 재구성과 탐지를 수행한다.

NovelADS 시스템은 기존 방법에 비해 정확도, 속도, 새로운 공격에 대한 견고성 측면에서 우수한 성능을 나타낸다. 차량에 이 시스템을 구현함으로써 공격을 조기에 탐지하고 차량 기능 결함으로 인한 사고를 예방하는 데 도움이 되며, 일반적인 이상 탐지 시나리오에 효과적인 해결책을 제시한다.

Ⅴ. 결 론

본 논문은 차량 네트워크 공격 대응을 위해 가상화 사이버 훈련 개발환경과 차량 In-vehicle 공격 및 탐지 유즈케이스를 조사했다. 현대 사회에서 인터넷 기술이 발전함에 따라 사이버 공격과 보안 위협이 증가하고 있다. 특히 자율주행차는 기계와 전자기기의 복잡한 상호작용으로 이루어져 있으며, 이로 인해 이기종 네트워크와 고도의 보안체계를 고려한 특별한 가상화 사이버 훈련 환경이 필요하다. 또한 실제 물리적인 실험 환경에서 사이버 훈련을 진행하는 것은 교통사고

및 안전사고 위험이 존재하므로, 가상화 사이버 훈련 시스템이 필요하다. 가상화 사이버 훈련 과정은 자율주행차 보안전문가를 양성하기 위한 실험 환경과 네트워크 인터페이스를 제공하는데 높은 비용과 접근 장벽을 극복하는데 기여할 수 있다. 그러므로 본 논문은 가상화 사이버 훈련장을 개발하고자 하는 연구자의 빠른 이해에 도움이 될 것이다.

참 고 문 헌.

[1] Lee, Daesung. "The Trends of Domestic and Overseas Cyber Security Training." Journal of the Korea Institute of Information & Communication Engineering 25.6 (2021).

[2] 최영한, et al. "사이버 위기 경보 기반 사이버 방어 훈련장 설계 및 구축 연구." 정보보호학회논문지 30.5 (2020): 805-821.

[3] Trickel, Erik, et al. "Shell We Play A Game?{CTF-as-a-service} for Security Education." 2017 USENIX Workshop on Advances in Security Education (ASE 17). 2017.

[4] Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos. "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture." Computers & Security 88 (2020): 101636.

[5] Pihelgas, Mauno. "Design and implementation of an availability scoring system for cyber defence exercises." Proceedings of the 14th International Conference on Cyber Warfare and Security. 2019.

[6] Oesch, Sean, et al. "D2u: Data driven user emulation for the enhancement of cyber testing, training, and data set generation." Cyber Security Experimentation and Test Workshop. 2021.

[7] Kim, Donghwa, et al. "Automated cyber threat emulation based on ATT&CK for cyber security training." Journal of the Korea Society of Computer and Information 25.9 (2020): 71-80.

[8] Standen, Maxwell, et al. "Cyborg: A gym for the development of autonomous cyber agents." arXiv preprint arXiv:2108.09118 (2021).

[9] Lee, Donghwan, et al. "Cy-through: toward a cybersecurity simulation for supporting live, virtual, and constructive interoperability." IEEE Access 9 (2021): 10041-10053.

[10] Zilberman, Polina, et al. "Sok: A survey of open-source threat emulators." arXiv preprint arXiv:2003.01518 (2020).

[11] Jo, Hyo Jin, and Wonsuk Choi. "A survey of attacks on controller area networks and corresponding countermeasures." *IEEE Transactions on Intelligent Transportation Systems* 23.7 (2021): 6123-6141.

[12] Lo, Wei, et al. "A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic." *Vehicular Communications* 35 (2022): 100471.

[13] Zhao, Yilin, Yijie Xun, and Jiajia Liu. "ClockIDS: A real-time vehicle intrusion detection system based on clock skew." *IEEE Internet of Things Journal* 9.17 (2022): 15593-15606.

[14] Agrawal, Kushagra, et al. "NovelADS: A novel anomaly detection system for intra-vehicular networks." *IEEE Transactions on Intelligent Transportation Systems* 23.11 (2022): 22596-22606.

〈저 자 소 개〉

김 호 준 (Hojun Kim)

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

<관심분야> 자동차 보안, 시스템 보안, 정보보호

최 영 호 (YongHo Choi)

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

<관심분야> 자동차 보안, 시스템 보안, 정보보호

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

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 인공지능사이버 보안학과 산학협력중점교수

2022년 9월~현재 : 고려대학교 인공지능사이버 보안학과 조교수

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