논문 2026-1-6 http://dx.doi.org/10.29056/jsf.2026.03.06

AI 학습기반 네트워크 공격대응 시스템 설계

김완태*†

Design of AI-Based Network Attack Response System

Wan-Tae Kim*†

요 약

최근 다양한 분야에서의 네트워크 사용이 증가되고 있으며, 산업 전반에 걸쳐 네트워크 사용에 대한 의존도가 높아지고 있다. 하지만 네트워크 사용 확대에 따른 다양한 부작용도 함께 증가하고 있으며 그중 네트워크 성능을 저하시키는 DoS, DDoS, UDP Flooding 공격에 따른 문제가 심각해지고 있다. 본 논문에서는 이러한 문제를 해결하기 위해 NS-3 기반 가상 네트워크 환경에서 DoS, DDoS, UDP Flooding 공격을 재현하고 IDS 탐지 성능을 분석한다. 탐지 로그는 CSV 파일 기록을 이용해 TensorFlow 기반 강화학습을 통해 정탐률을 향상시키고 오탐률을 감소시킬 수 있도록 설계하였으며, 인공지능(Explainable AI, XAI) 기법을 활용하여 탐지 과정을 시각화함으로써 모델 판단 근거의 투명성을 확보하였다. 특히 학습된 모델과 실시간 알람 기능을 연동하여 비정상 패턴 탐지, 즉시 운영자에게 경보를 전송하도록 설계하였다.

Abstract

Recently, network usage has increased across various sectors, and the level of dependence on network infrastructure throughout industry has grown significantly. However, alongside this expansion, various adverse effects have also risen, among which performance-degrading attacks such as DoS, DDoS, and UDP Flooding have become increasingly severe. In this paper, to address these issues, DoS, DDoS, and UDP Flooding attack scenarios were reproduced in an NS-3-based virtual network environment, and the detection performance of an Intrusion Detection System (IDS) was analyzed. Detection logs were recorded in CSV format and utilized to design a TensorFlow-based reinforcement learning model aimed at improving the true positive rate while reducing the false positive rate. Furthermore, Explainable Artificial Intelligence (XAI) techniques were applied to visualize the detection process, thereby ensuring transparency in the model's decision-making rationale. In particular, the trained model was integrated with a real-time alert mechanism so that operators would receive immediate notifications upon detection of abnormal patterns.

한글키워드 : 탐지로그, NS-3, 패턴탐지, 실시간, 알람

keywords : detection log, NS-3, pattern detection, real-time, alert

1. 서 론

기술의 급속한 발전과 함께 사이버 공격은 더욱 지능화·정교화되고 있으며, 그 영향력 또한 일

* 서일대학교
† 교신저자: 김완태(email:wtkim@seoil.ac.kr)
접수일자: 2026.02.25. 심사완료: 2026.03.14.
게재확정: 2026.03.20.

상 전반으로 빠르게 확산되고 있다. 특히 2025년에는 사회공학적 기법과 네트워크 보안의 취약점을 악용한 해킹 공격이 활발히 탐지되고 있으며, 침해 및 피해 사례 역시 지속적으로 증가하는 추세이다[1]. 이 가운데 서비스 거부 공격(DoS), 분산 서비스 거부 공격(DDoS), UDP Flooding과 같은 대량 트래픽 유발 공격은 네트워크 성능을 저하시킬 뿐 아니라 서비스 가용성을 심각하게 위협하는 대표적 공격 유형으로 지목되고 있다 . 이러한 공격은 단시간 내 대규모 트래픽을 발생시키기 때문에 기존의 패턴(Signature) 기반 침입탐지시스템(IDS)만으로는 신속하고 정확한 대응에 한계가 있다[2][3]. IDS는 네트워크 보안 체계에서 핵심적인 방어 수단으로서 악성 트래픽 및 비정상 행위를 탐지·분석하는 역할을 수행하지만 전통적인 IDS는 높은 False Positive Rate과 False Negative Rate의 문제를 동시에 내포하고 있으며, 알려지지 않은 신종 공격에 대한 대응 능력 또한 제한적이다. 따라서 단순한 규칙 또는 시그니처 업데이트 중심의 개선만으로는 고도화되는 사이버 위협에 효과적으로 대응하기 어려운 실정이다[3].

본 논문에서는 NS-3 기반 가상 네트워크 환경을 구축하고 DoS, DDoS, UDP Flooding 공격 시나리오를 체계적으로 재현하여 IDS의 탐지 성능을 분석한다[4]. 수집된 탐지 로그는 CSV 파일 형태로 저장·관리되며, TensorFlow 기반 강화학습(Reinforcement Learning) 기법을 적용하여 정탐률(True Positive Rate)을 향상시키고 오탐률(False Positive Rate)을 감소시키는 방향으로 탐지 성능을 최적화하였다[5][6]. 또한 설명 가능한 인공지능(Explainable AI, XAI) 기법을 활용하여 IDS의 탐지 의사결정 과정을 시각화하고 모델의 판단 근거를 분석함으로써 탐지 결과의 투명성과 신뢰성을 확보하고자 하였다.

따라서, 강화학습 기반 탐지 과정에 실시간 알람 전송(Real-Time Alerting) 기능을 통합하여 IDS가 비정상 패턴을 탐지하는 즉시 운영자에게 경보가 전달되도록 설계하였고, 이를 통해 학습된 탐지 모델이 단순 성능 향상 수준을 넘어 실제 보안 운영 환경에서도 즉각적이고 효율적인 대응 체계를 지원할 수 있도록 설계하였다.

2. 본 론

2.1 침입 탐지 시스템(IDS)

NS-3(Network Simulator 3)는 패킷 단위(Packet-level) 네트워크 동작을 정밀하게 모델링할 수 있도록 설계된 이벤트 기반(Event-driven) 오픈소스 네트워크 시뮬레이터로, 유·무선 네트워크 프로토콜 분석과 보안 성능 평가 연구에 폭넓게 활용되고 있다. NS-3는 실제 인터넷 프로토콜 스택과 유사한 구조를 제공하며, TCP/IP, UDP, 라우팅 프로토콜, 트래픽 제어, 링크 특성 등을 세부적으로 설정할 수 있어 현실성 높은 가상 네트워크 환경 구축이 가능하다. 또한 C++ 기반 코어와 Python 바인딩을 함께 지원하여 확장성과 실험 자동화 측면에서도 높은 활용성을 가진다.

NS-3를 활용한 침입탐지시스템(IDS) 성능 평가 연구에서는 다양한 네트워크 토폴로지(Topology)와 공격 시나리오를 유연하게 구성할 수 있다. 서버-클라이언트 구조, 다중 라우터 환경, 대규모 노드 기반 분산 네트워크 등을 모델링하고, DoS, DDoS, UDP Flooding과 같은 트래픽 기반 공격을 재현함으로써 IDS의 탐지 반응을 정밀하게 측정할 수 있다. 특히 시뮬레이션 과정에서 생성되는 모든 패킷 흐름과 이벤트 정보는 로그 데이터로 수집되며, 이는 탐지 알고리즘 학습 및 성능 분석의 기초 자료로 활용된다. 논문에서 구성한 IDS 시뮬레이션 환경은 크게 트래픽 생성

부, 공격 시나리오 모듈, 탐지 엔진, 로그 수집 및 분석부로 구성된다. 먼저 정상 트래픽과 공격 트래픽을 동시에 생성하여 실제 네트워크와 유사한 부하 환경을 조성한다. 공격 시나리오 모듈에서는 트래픽 발생 주기, 패킷 크기, 전송 속도, 공격 노드 수 등을 조정하여 다양한 강도의 공격 패턴을 구현한다. 탐지 엔진은 네트워크 구간에서 수집된 패킷 특성 정보를 기반으로 비정상 행위를 식별하며, 탐지 결과는 CSV 형식의 로그로 저장된다. 이와 같이 NS-3 환경에서 구현된 IDS는 정탐률(True Positive Rate), 오탐률(False Positive Rate), 미탐률(False Negative Rate)과 같은 핵심 성능 지표를 기준으로 정량적 평가가 가능하다. 또한 동일 조건에서 탐지 알고리즘별 성능을 반복 비교할 수 있어 IDS 모델의 신뢰성과 재현성을 확보할 수 있다. NS-3는 실제 네트워크 인프라를 물리적으로 구축하지 않고도 대규모 공격 실험과 다양한 보안 시나리오 검증이 가능하다는 점에서 비용 및 시간 절감 측면에서도 높은 효율성을 제공한다. 최근 IDS 연구에서는 단순 탐지 기반을 넘어 머신러닝 및 강화학습 기반 접근을 통해 탐지 성능 향상을 검증하기 위해 사용되고 있다[7-10]. 기존 연구에서는 TensorFlow와 같은 딥러닝 프레임워크를 활용하여 네트워크 트래픽 분석 및 이상 패턴 탐지 모델을 학습시키고 정탐률, 오탐률, 미탐률과 같은 성능 지표를 기반으로 모델 성능을 평가하였다[5]. 그러나 기존 연구에서 실시간 알람 기능과의 통합 사례는 제한적이며, 대부분 모델 학습과 평가 단계에 초점이 맞춰져 있다. 따라서, 본 논문에서는 학습된 강화학습 기반 IDS 모델과 실시간 알람 시스템을 연동하여 비정상 패턴 탐지 시 즉시 경보를 발송하도록 설계하였다. 이를 통해 모델이 단순 탐지 성능 향상에 그치지 않고 실시간 보안 대응까지 가능하도록 구현하였다.

2.2 AI(XAI)를 활용한 IDS 신뢰성 강화

설명 가능한 인공지능(Explainable AI, XAI)은 IDS의 의사결정 과정을 시각화하고 모델 판단 근거를 분석할 수 있게 함으로써 탐지 결과의 투명성과 신뢰성을 높이는 데 활용된다. 기존 IDS는 높은 탐지 성능에도 불구하고 탐지 결과가 블랙박스(Black-box) 형태로 제공된다는 한계로 인해 관리자 신뢰성 확보와 정책 반영 과정에서 어려움이 존재하였다. 특히, 탐지 원인을 명확히 설명하지 못할 경우 오탐(False Positive)에 대한 대응 지연이나 보안 정책 오류로 이어지고 있다. 따라서, 논문에서 제시하는 XAI 기반[11] 접근은 각 트래픽 이벤트가 공격으로 분류된 이유에 대하여 중요도(Feature Importance), 기여도 분석, 시각화 그래프 등의 형태로 제시함으로써 모델의 판단 근거를 직관적으로 이해할 수 있도록 지원하며, 이를 통해 관리자와 운영자는 IDS 탐지 결과를 신속히 해석하고 상황에 적합한 대응 전략을 수립할 수 있으며, 보안 정책의 정밀도 또한 향상될 수 있도록 설계하였다. 인공지능(AI) 기반 IDS는 대규모 네트워크 트래픽을 실시간으로 학습·분석할 수 있어 기존 규칙 기반 시스템 대비 탐지 정확도와 확장성을 개선하였다[12][13]. 새로운 공격 패턴이 발생하더라도 지속적인 학습을 통해 스스로 탐지 기준을 갱신할 수 있으며, 변종 및 미지 공격(Zero-day Attack)에 대한 대응 가능성도 개선할 수 있다. 또한 자동화된 위협 분류와 우선순위 분석 기능을 통해 보안 인력의 운영 부담을 경감시키고, 대응 시간 단축 및 보안 운영 효율성 향상에 기여할 수 있다. 따라서 XAI를 결합한 AI 기반 IDS는 단순 탐지 성능 개선을 넘어 탐지 결과의 해석 가능성, 운영 신뢰성, 대응 의사결정 지원 측면에서 통합적 보안 운영 역량을 강화하는 핵심 기술로 활용될 수 있다[14][15].

3. 시스템 설계

3.1 시스템 아키텍처

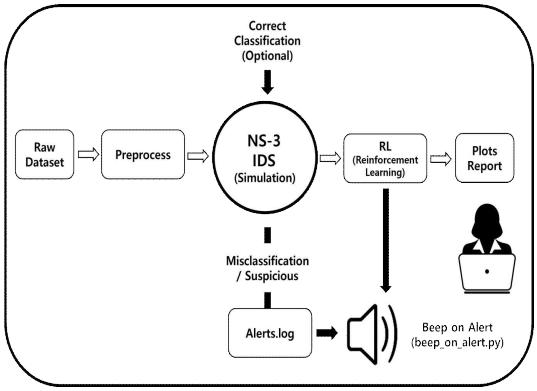

그림 1. 제안하는 시스템 구성도
Fig. 1. Proposed system architecture

가상 네트워크 환경에서 다양한 서비스 거부 공격을 재현하고 이를 지능적으로 탐지·대응하기 위한 통합형 침입탐지시스템(IDS) 아키텍처는 그림 1과 같다. NS-3 기반 시뮬레이션 환경을 중심으로 설계하였으며, 정상 트래픽과 공격 트래픽이 혼재된 실제 네트워크 상황을 모사할 수 있도록 구성되었다. 특히 DoS, DDoS, UDP Flooding 공격 시나리오를 구현하여 단일 공격뿐 아니라 분산 환경에서 발생하는 대규모 트래픽 공격도 적용하였고, 이러한 구조는 시뮬레이션의 재현성과 확장성을 동시에 확보하면서도 실제 운영 환경과 유사한 조건에서 IDS 성능을 평가할 수 있다. 트래픽 생성 모듈은 정상 패킷과 공격 패킷을 혼합하여 전송하도록 설계되었으며, 이를 통해 단순 패턴 기반 탐지 환경이 아닌 복합 트래픽 상황을 구성한다. IDS 모듈은 네트워크 흐름을 실시간으로 모니터링하면서 비정상 트래픽 여부를 판단하고, 탐지 결과를 CSV 형식의 로그 파일로 기록한다. 이 로그에는 트래픽 특징값, 예측 결과, 예측 확률, 시간 정보 등이 포함되며, 이는 후속 학습 및 성능 분석 단계에서 활용된다. 즉, 본 시스템은 실시간 탐지 기능과 학습 데이터 축적 기능을 동시에 수행하는 구조를 가진다. 강화학습 기반 에이전트는 기록된 로그 데이터를 기반으로 상태와 행동을 정의하고, 탐지 결과에 따른 보상을 통해 정책을 학습한다. 보상 함수는 TPR(True Positive Rate)을 최대화하고 FPR(False Positive Rate)을 최소화하는 방향으로 설계되었으며, 이를 통해 공격 탐지율을 유지하면서도 오탐률을 낮추는 균형 잡힌 정책을 도출한다. 이러한 동적 정책 학습 구조는 고정 임계값 기반 IDS의 한계를 보완하며, 네트워크 환경 변화에 적응 가능한 지능형 탐지 체계를 구현하였다. 또한, 본 연구는 탐지 결과의 해석 가능성과 신뢰성 확보를 위해 설명 가능한 인공지능(XAI) 모듈을 통합하였으며, 기존 IDS는 높은 탐지 성능을 보이더라도 판단 근거가 불투명하다는 문제가 있었으나, 제안 시스템은 모델이 특정 트래픽을 공격으로 판단한 주요 특징과 중요도를 시각화하여 제공한다. 이를 통해 운영자는 탐지 결과의 근거를 직관적으로 이해할 수 있으며, 오탐 발생 시 원인 분석과 정책 개선이 가능해진다. 결과적으로 탐지 정확성뿐 아니라 투명성과 신뢰성을 동시에 확보할 수 있다. 비정상 트래픽이 탐지될 경우 실시간 알람 모듈이 즉시 동작하여 운영자에게 경보를 전송하도록 설계하였고, 이는 단순히 로그를 기록하는 수동적 시스템이 아니라, 탐지와 동시에 대응이 가능한 능동형 보안 체계를 구현하기 위함이다. 실시간 경보 구조는 관리자의 즉각적인 개입을 가능하게 하며, 추가적인 대응 시스템과의 연동 또한 확장 가능하도록 설계되었다. 그림 1 시스템 블록도에서 나타난 바와 같이, 본 아키텍처는 공격 재현, 실시간 탐지, 로그 축적, 정책 학습, 설명 제공, 경보 전송의 일련의 과정을 유기적으로 통합한 순환 구조를 형성하였으며, 제안된 IDS 시스템은 탐지

성능, 적응성, 설명 가능성, 실시간 대응성을 동시에 고려한 통합 지능형 보안 프레임워크로의 의미를 가질 수 있도록 구현하였다.

3.2 학습 모델 및 알고리즘

강화학습 모델의 입력에 해당하는 상태(State)는 네트워크 트래픽 정보와 IDS의 탐지 결과로 구성되며, 패킷 및 흐름 정보와 같은 네트워크 특징뿐 아니라, 해당 트래픽이 공격인지 정상인지에 대한 판단 결과와 탐지 신뢰도에 대한 XAI 기반 정보를 포함하였다. 현재 네트워크의 상태를 바탕으로 강화학습 에이전트는 대응 행동(Action)을 선택하게 되며. 행동은 주로 정상 트래픽 허용, 의심 트래픽 차단, 그리고 추가적인 검사를 수행하는 방식으로 구성된다. 실제 운영 환경에서 필요한 대응 정책을 결정하는 과정에 대한 모델링과 보상(Reward)은 시스템 성능을 결정짓는 중요한 요소로, IDS의 성능 지표인 TPR과 FPR을 기반으로 설계 하였다. 공격을 정확하게 탐지하고 차단할 경우에는 높은 보상이 주어지며, 정상 트래픽을 잘못 차단하는 경우에는 큰 패널티가 부여된다. 또한 공격을 놓치는 경우에도 부정적인 보상이 주어지도록 구성되어, 탐지 정확도와 오탐 최소화를 동시에 고려하도록 하였다. 이러한 구조를 바탕으로 강화학습은 상태-행동-보상 간의 반복적인 상호작용을 통해 최적의 정책을 학습하게 제안하였다. IDS가 네트워크 상태를 제공하면 에이전트가 대응 행동을 선택하고, 그 결과에 따라 보상을 받은 뒤 정책을 업데이트하는 과정이 지속적으로 반복된다. 이러한 학습 과정을 통해 시스템은 점차 다양한 상황에서 가장 효과적인 대응 전략을 스스로 도출할 수 있게 된다. XAI 결과를 시각적으로 표현하기 위해 사용한 시각화 라이브러리는 matplotlib과 seaborn을 사용하였으며, 데이터 분포, 특징 중요도, 그리고 결과를 그래프 형태로 표현을 통해 논문에서 제시한 성능 평가 지표인 TPR과 FPR, 그리고 보상 변화 추이를 시각화하였다. 데이터 처리 및 분석을 위해서는 pandas와 numpy를 사용하였으며, pandas의 사용은 네트워크 트래픽 데이터와 같은 구조화된 데이터를 효율적으로 처리하고 분석하는 데 적합하며, numpy는 수치 연산 및 행렬 계산을 위해 사용하였다. IDS 성능 평가를 위한 TPR, FPR 등의 지표 계산이나 기본적인 머신러닝 모델 활용을 위해 scikit-learn을 적용하였다.

3.3 시뮬레이션 조건, IDS 탐지 메트릭, 보상

시뮬레이션 환경은 NS-3 기반 가상 네트워크 상에서 정상 트래픽과 공격 트래픽이 공존하는 구조로 설계하였으며, 실험 환경은 서비스 거부(DoS), 분산 서비스 거부(DDoS), UDP Flooding 공격을 재현할 수 있도록 구성하였다. 네트워크 계층에서의 트래픽 흐름과 패킷 단위 동작을 정밀하게 관찰할 수 있도록 설정하였고, 공격시나리오 및 트래픽 모델링은 다음과 같은 파라미터를 이용하여 설정하였다.

```
// 공격 트래픽 (OnOffApplication: UDP Flooding, DDoS,
// DoS)
uint16_t port = 9;  // 공격 대상 포트
OnOffHelperonoff("ns3::UdpSocketFactory",
InetSocketAddress(i.GetAddress(1), port));
onoff.SetAttribute("DataRate",StringValue("50Mbps"));
onoff.SetAttribute("PacketSize", UintegerValue(1024));
ApplicationContainer attackApps =
onoff.Install(nodes.Get(0)); attackApps.Start(Seconds(1.0));
attackApps.Stop(Seconds(10.0));
// 정상 트래픽 (PacketSinkApplication)
PacketSinkHelpersink("ns3::UdpSocketFactory",
InetSocketAddress(Ipv4Address::GetAny(), port));
ApplicationContainer sinkApps = sink.Install(nodes.Get(1));
sinkApps.Start(Seconds(0.0));
sinkApps.Stop(Seconds(15.0));
```

공격 트래픽은 NS-3의 OnOffApplication을 활용하여 구현하였으며, 전송 프로토콜은 UDP 소켓을 사용하였다. 임의의 목적지 포트 9를 공격 대상으로 설정하였고, 전송률(DataRate)은 50 Mbps로 구성하여 고속 대량 패킷 전송 환경을 가정하였고, 패킷 크기(PacketSize)는 1024 Byte로 설정하여 실제 UDP Flooding 공격과 유사한 트래픽 특성을 반영하였다. 공격 애플리케이션은 시뮬레이션 시작 후 1초 시점부터 동작하도록 설정하고, 10초 시점에 종료되도록 구성하였다. 이를 통해 정상 구간(0~1초), 공격 구간(1~10초), 공격 종료 후 안정화 구간(10~15초)을 구분하여 탐지 성능 변화를 분석할 수 있도록 하였다. DDoS 시나리오의 경우에는 다수의 노드에서 동일 설정의 OnOffApplication을 동시에 실행함으로써 분산 공격 환경을 가정하였다. 정상 트래픽 수신을 위해 PacketSinkApplication을 동일한 UDP 포트 9에 설치하였다. PacketSink는 모든 인터페이스(Ipv4Address::GetAny())로부터 수신되는 패킷을 기록하도록 설정하여 공격 및 정상 트래픽을 모두 수집할 수 있도록 하였으며, 해당 애플리케이션은 시뮬레이션 시작 시점인 0초부터 동작하도록 설정하고, 전체 시뮬레이션 종료 시점인 15초까지 유지함으로써 전 구간의 트래픽을 안정적으로 수집하도록 설계하였다. 이와 같은 시뮬레이션 구성은 일정 시간 동안 집중적으로 발생하는 고강도 UDP 기반 공격 트래픽이 네트워크에 미치는 영향을 분석하고, IDS 모듈이 공격 발생 구간을 정확히 식별하는지 평가하기 위한 목적을 가진다. 또한 시간 구간을 명확히 구분함으로써 탐지율(True Positive Rate), 오탐률(False Positive Rate), 탐지 지연 시간 등을 정량적으로 측정할 수 있도록 하였다.

강화학습 기반 정책을 사용하여 IDS의 실시간 탐지 성능을 최적화한다. 정책이 선택한 행동은 NS-3 시뮬레이션에 적용되어 트래픽 결과를 CSV로 기록한다. 이를 통해 정탐률, 오탐률, 정상 트래픽 품질 손실(QoS)을 계산한다. 각 항목의 계산은 표 1과 같다.

표 1. IDS 탐지 메트릭 및 보상
Table 1. IDS detection metrics and rewards

항목	계산 / 값
TPR (정탐률)	TPR = TP/(TP + FN)
FPR (오탐률)	FPR = FP / (FP + TN)
QoS 손실	QoS = max(0,(link - benign_mean)/link)
Reward (보상)	Reward = TPR - FPR - 0.2 * QoS

4. 실험 및 결과

4.1 TPR_FPR 결과

본 논문에서 제시한 시스템의 시뮬레이션 결과 DDoS, DoS, UDP 공격 모두 초기 에피소드 구간에서 TPR이 점진적으로 상승하는 학습 곡선을 보였으며, 에피소드가 진행될수록 수렴 구간에 도달하면서 비교적 안정적인 값을 유지하는 형태를 나타냈다. 이는 강화학습 기반 정책이 반복 학습을 통해 공격 탐지 정확도를 점차 향상시키는 것을 알 수 있다.

1차 시도의 경우, DDoS 공격은 초기 1~5 에피소드 구간에서 일부 점들이 상대적으로 높은 위치에 분포하며 다소 변동성이 존재하는 모습을 보였다. 이는 초기 탐지 정책이 완전히 안정화되지 않은 상태에서 탐지율이 일시적으로 높게 나타났음을 의미한다. 반면 5차 시도에서는 동일 구간에서 점의 위치가 소폭 낮아지고 분포가 균등해지면서 과도한 변동이 줄어든 양상을 확인할 수 있다. 이는 반복 실험을 통해 초기 학습 단계의 불안정성이 완화되고, 보다 안정적인 정책 수렴이 이루어졌음을 보여준다. DoS 공격의 경우

40~50 에피소드 구간에서 1차 시도의 평균 TPR은 약 0.92~0.93 수준으로 나타났으며, 5차 시도에서는 약 0.91~0.92 수준으로 소폭 감소하였다.

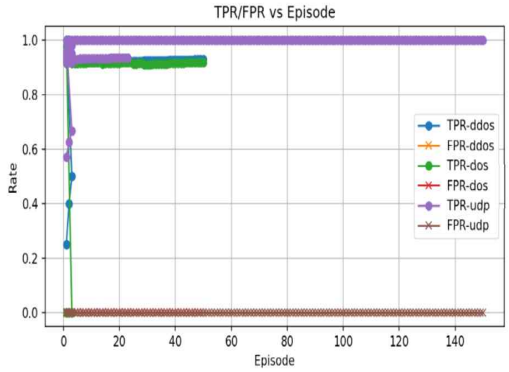

그림 2. 1차 시도 line_TPR_FPR
Fig. 2. line_TPR_FPR of the First Trial

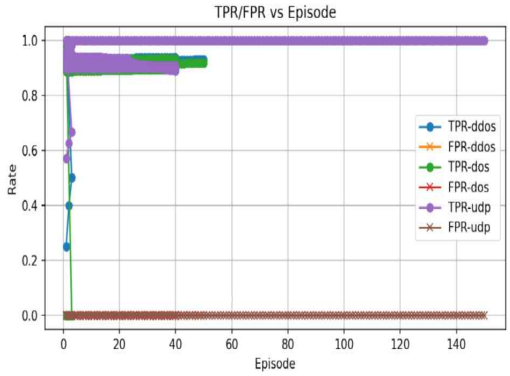

그림 3. 5차 시도 line_TPR_FPR
Fig. 3. line_TPR_FPR of the Fifth Trial

절대적인 탐지율은 약간 낮아졌으나, 전체적인 점 분포는 더욱 일정하게 정렬되는 경향을 보였다. 이는 극단적인 탐지율 상승보다는 안정적인 평균 성능 유지에 초점을 둔 정책 조정이 이루어졌음을 알 수 있다. UDP 공격은 가장 뚜렷한 학습 수렴 특성을 보였으며, 초기 에피소드 에서 약 0.6 수준의 TPR로 시작하였으나, 에피소드가 진행됨에 따라 0.95~0.99 수준까지 빠르게 상승하였다. 최종 수렴 값은 1차와 5차 시도 모두 거의 동일하게 유지되었으며, 이는 UDP 유형에 대한 탐지 정책이 비교적 빠르게 학습되고 안정적으로 수렴함을 의미한다. 특히 5차 시도에서는 점 분포가 보다 균등하게 배열되어 변동 폭이 감소한 것으로 나타났다. FPR 측면에서도 전반적으로 학습이 진행됨에 따라 감소 또는 안정화되었으며, 5차 시도에서는 초기 구간의 변동 폭이 줄어들어 오탐률 관리 측면에서도 안정성이 향상된 것을 확인할 수 있다. 따라서, 1차 시도는 탐지율이 빠르게 상승하는 특성을 보이나 초기 변동성이 존재하였으며, 5차 시도에서는 평균 TPR이 일부 구간에서 소폭 낮아진 대신, 점 분포가 균등하게 정렬되어 전반적인 학습 안정성이 향상된 것으로 나타났다. 이는 강화학습 기반 IDS 정책이 반복 학습을 통해 과도한 편차를 줄이고, 안정적이고 신뢰 가능한 탐지 성능으로 수렴하고 있음을 알 수 있다.

4.2 Reward 결과

DDoS, DoS, UDP 공격에서 초기 에피소드를 제외하면 보상 값은 약 0.78~0.82 구간에 집중되어 나타났으며, 학습이 진행됨에 따라 일정 범위 내에서 안정적으로 유지되는 경향을 보였다. 이는 강화학습 기반 IDS 정책이 반복 학습을 통해 급격한 보상 변동 없이 수렴 구간에 도달했음을 확인할 수 있다.

1차 시도의 경우 DoS와 DDoS 공격에서 보상 점들의 분포가 다소 분산되어 나타났으나, 동일한 에피소드 구간 내에서도 점 간 간격이 일정하지 않고, 일부 구간에서는 미세한 변동이 반복되는 양상을 보였다. 이는 초기 학습 단계에서 정책이 완전히 안정화되지 않아 보상 값의 변동성이 존재했을 것으로 예상할 수 있다. 반면 5차 시도에서는 동일한 보상 범위(0.78~0.82) 내에서 점들이 보다 조밀하게 모여 분포하였으며, 전체

적인 분산이 감소한 모습을 확인할 수 있다. 이는 반복 실험을 통해 안정화와 일관성을 향상되는 것을 확인할 수 있다.

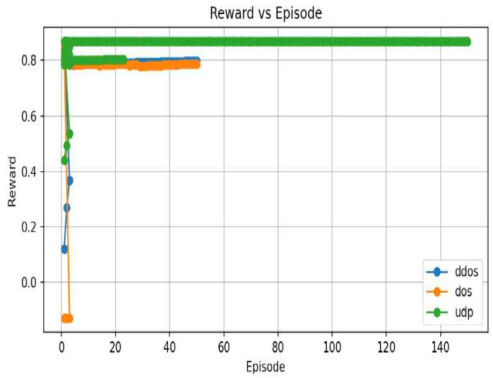

그림 4. 1차 시도 line_reward
Fig. 4. line_reward of the First Trial

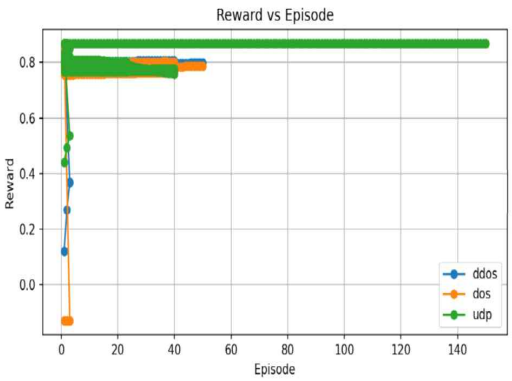

그림 5. 5차 시도 line_reward
Fig. 5. line_reward of the Fifth Trial

UDP 공격의 경우 plateau 구간의 위치 변화가 비교적 명확하게 나타났으며. 1차 시도에서는 보상 값이 약 0.84~0.86 범위에서 형성되었으나, 5차 시도에서는 0.85~0.87 수준으로 소폭 상승하였다. 이는 UDP 유형에 대한 최적화가 반복 학습을 통해 더욱 향상된 것을 확인할 수 있다. 초반 에피소드에서 나타나는 outlier 분포는 1차부터 5차 시도까지 유사하게 관찰되었으나, 5차 시도에서는 해당 구간 이후 보상 값이 빠르게 안정 구간으로 수렴하였다. 결과적으로 전체 보상 분포의 균형성과 일관성이 향상되었으며, 학습 누적 효과와 데이터 정렬 개선이 보상 안정화에 긍정적인 영향을 미친 것으로 분석된다. 5차 시도에서는 평균 보상 값이 유지되거나 일부 유형에서 소폭 상승하는 동시에, 분산이 감소하고 점 분포가 균등하게 정렬되는 특성을 보였다. 이는 강화학습 기반 IDS 정책이 반복 학습을 통해 점진적으로 안정화되고 있음을 보여주는 결과이며, 향후 학습 시도를 추가로 확대할 경우 더욱 높은 정책 안정성과 성능 일관성을 확보할 수 있을 것으로 예상된다.

5. 결 론

본 논문에서는 NS-3 기반 가상 네트워크 환경에서 다양한 DoS, DDoS, UDP Flooding 공격 시나리오를 재현하고, 강화학습 기반 IDS 아키텍처의 성능을 체계적으로 분석하였다. 정상·공격 트래픽이 혼재된 환경에서 실시간 탐지, 로그 축적, 정책 학습, 설명 제공, 경보 전송까지 통합한 구조를 설계함으로써 기존 패턴 기반 IDS의 한계를 보완할 수 있도록 시스템을 설계하였으며, TensorFlow 기반 강화학습 기법을 적용하여 TPR(True Positive Rate)과 FPR(False Positive Rate)을 동시에 최적화하는 정책을 학습하도록 설계하였고, 시뮬레이션을 통해 학습 안정성과 수렴 특성을 확인하였다. 실험 결과, 제안한 IDS는 일부 시도에서 정탐률 100%, 오탐률 0%에 근접하는 성능을 달성하였다. 이는 고정 임계값이나 시그니처 기반 탐지 방식과 달리, 환경 변화에 적응하는 동적 정책 학습 구조가 효과적으로 작동했음을 확인할 수 있었고, 에피소드가 누적될수록 TPR과 보상 분포가 안정적으로 수렴하

고, 점 분포의 분산이 감소하는 것을 확인함으로써 학습 안정성이 향상됨을 확인하였다. UDP 유형에서는 빠른 수렴 특성이 나타났으며, DDoS 및 DoS 유형에서도 반복 학습을 통해 변동성이 점차 완화되었다.

실시간 알람 기능을 통해 비정상 패턴 탐지 시 즉시 경보가 발송되도록 설계함으로써 단순 탐지 시스템을 넘어 능동적 대응이 가능한 보안 체계를 구현하였고, 이는 실제 운영 환경에서 탐지 지연을 최소화하고 신속한 대응을 가능하게 할 수 있다. 인공지능(XAI) 기법을 적용하여 모델의 판단 근거를 시각화하고 특징 중요도를 그래프 형태로 제시하였으며, 이를 통해 관리자는 IDS의 의사결정 과정을 직관적으로 이해할 수 있으며, 오탐 발생 시 원인 분석과 정책 개선이 용이 해질수 있으며, 탐지 성능뿐 아니라 신뢰성과 투명성 측면에서도 개선 효과를 확인하였다.

본 논문은 강화학습, 실시간 알람, XAI를 통합한 지능형 IDS 프레임워크를 제안하고 실험적으로 그 성능과 안정성을 검증하였으며, 향후 확장 연구를 통해 보다 범용적이고 실제 환경에 적용 가능한 차세대 IDS로 발전시킬 수 있을 것으로 기대된다.

참 고 문 헌

[1] AhnLab, “From Clop to BPFDoor: Major Cyber Threat Trends in 2025”, AhnLab Security Report, 2025, https://www.ahnlab.com

[2] N. Hariharasubramanian, “Signature Based IDS vs. Anomaly Based IDS: Understanding the Difference and Choosing the Best for Your Needs”, Fidelis Security, 2025, https://fidelissecurity.com

[3] Fortinet, “What Is an Intrusion Detection System (IDS)?”, Fortinet Resources, 2025, https://www.fortinet.com

[4] ns-3 Project, “What Is ns-3”, nsnam.org, 2025, https://www.nsnam.org

[5] M. A. Hossain, “Ensuring Network Security with a Robust Intrusion Detection System”, Array, 19, pp.100306, 2023, DOI: 10.1016/j.array.2023.100306

[6] K. Ren, et al., “MAHFSIDS: Reinforcement Learning-Based Real-Time Intrusion Detection System”, Journal of Big Data, 10(137), pp.1-20, 2023, DOI: 10.1186/s40537-023-00788-2

[7] Z. Xu, et al., “Deep Learning-Based Intrusion Detection Systems: A Survey”, arXiv, 2025, https://arxiv.org

[8] N. Singh, T. Bhatia, “Adaptive Intrusion Detection System Leveraging Dynamic Neural Models with Adversarial Learning for 5G/6G Networks”, arXiv, 2025, https://arxiv.org

[9] S. K. R. Mallidi, R. R. Ramisetty, “Advancements in Training and Deployment Strategies for AI-Based Intrusion Detection Systems in IoT: A Systematic Literature Review”, Discover Internet of Things, 2025, DOI: 10.1007/s43926-025-00000-x

[10] S. Chatterjee, et al., “Intrusion Detection System Using Deep Learning for Network Security”, arXiv, 2025, https://arxiv.org

[11] E. S. Shin, S. B. Kim, Y. J. Yoon, H. J. Jung, “XAI-Based Intrusion Detection System: Enhancing IDS Transparency Using SHAP”, Proceedings of the 2024 Korea Institute of Information Technology Summer Conference, pp.1077-1081, 2024

[12] S. Chatzimiltis, et al., “Interpretable Anomaly-Based DDoS Detection in AI-RAN with XAI and LLMs”, arXiv, 2025, https://arxiv.org

[13] “Evaluating Machine Learning-Based Intrusion Detection Systems with Explainable AI: Enhancing Transparency

and Interpretability", Frontiers in Computer Science, 2025, DOI: 10.3389/fcomp.2025.00000
[14] A. Hozouri, A. Mirzaei, M. Effatparvar, "A Comprehensive Survey on Intrusion Detection Systems with Advances in Machine Learning and Emerging Cybersecurity Challenges", Discover Artificial Intelligence, 2025, DOI: 10.1007/s44163-025-00000-x
[15] "Deep Learning for Intrusion Detection in Emerging Technologies: A Comprehensive Survey and New Perspectives", Artificial Intelligence Review, 2025, DOI: 10.1007/s10462-025-00000-x

저 자 소 개

김완태(Wan-Tae Kim)

2005.2 한국항공대학교 정보통신공학 석사
2011.2 한국항공대학교 정보통신공학 박사
2011.3-현재 : 서일대학교 조교수
<주관심분야> 네트워크시스템, 임베디드시스템, 자율주행자동차, 지능형네트워크