PORTFOLIO

이름	주 상 현
생년월일	1994. 09. 27
이메일	kidney94@naver.com
전화번호	010-7172-3817

Profile

- **Education**
  - **Hansung University [2021.03 ~ 2023.02]**
    - ✓ **Department of IT Convergence Engineering, M.S.**
    - ✓ **GPA : 4.13 / 4.5**
  - **Hansung University [2015.03 ~ 2021.02]**
    - ✓ **Department of Information & System Engineering, B.S.**
    - ✓ **GPA : 3.51 / 4.5**
- **Research Interest**
  - **System Engineering**
    - ✓ **Embedded System**
  - **Artificial Intelligence**
    - ✓ **Adversarial Attack Defense & Detection**
    - ✓ **DNN Accelerate**
- **Publications**
  - M.S. Kim, **S.H. Joo**, "Time-Constrained Adversarial Defense IoT Edge Devices through Kernel Tensor Decomposition and Multi-DNN Scheduling", **Sensors**, 22(15), 5896.
  - **주상현**, 김인모, 김명선, "소프트웨어 기반 임베디드 시스템용 적대적 공격 검출 시스템", **IEIE(전자공학회논문지)**, 59(7), 3-11.

PORTFOLIO

CONTENTS

Project 01.

다중 객체 추적 성능 알고리즘 분석

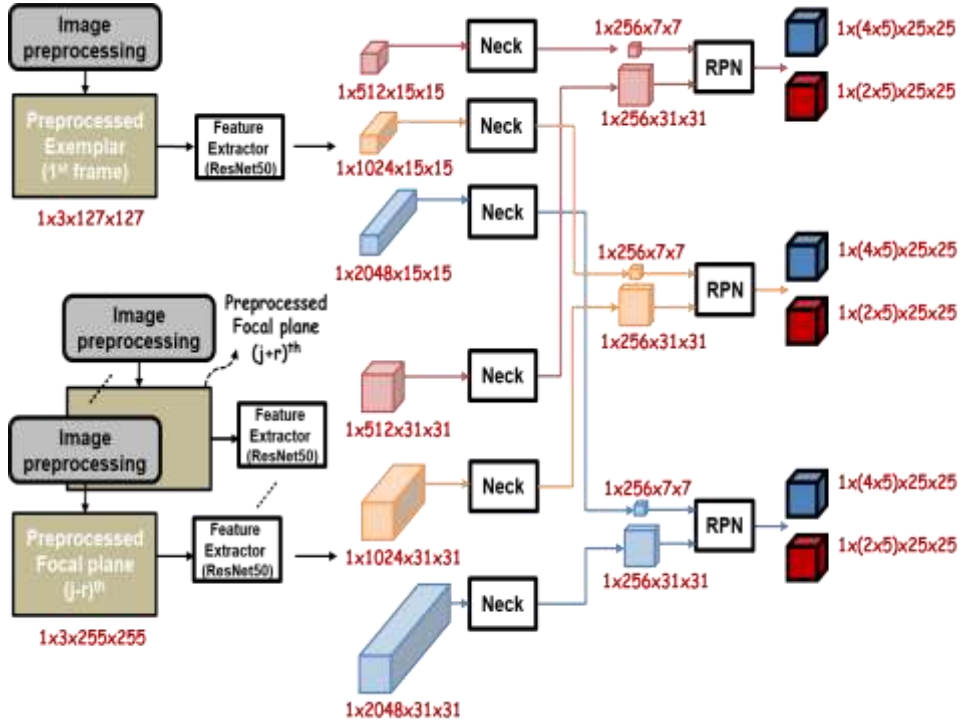
About project

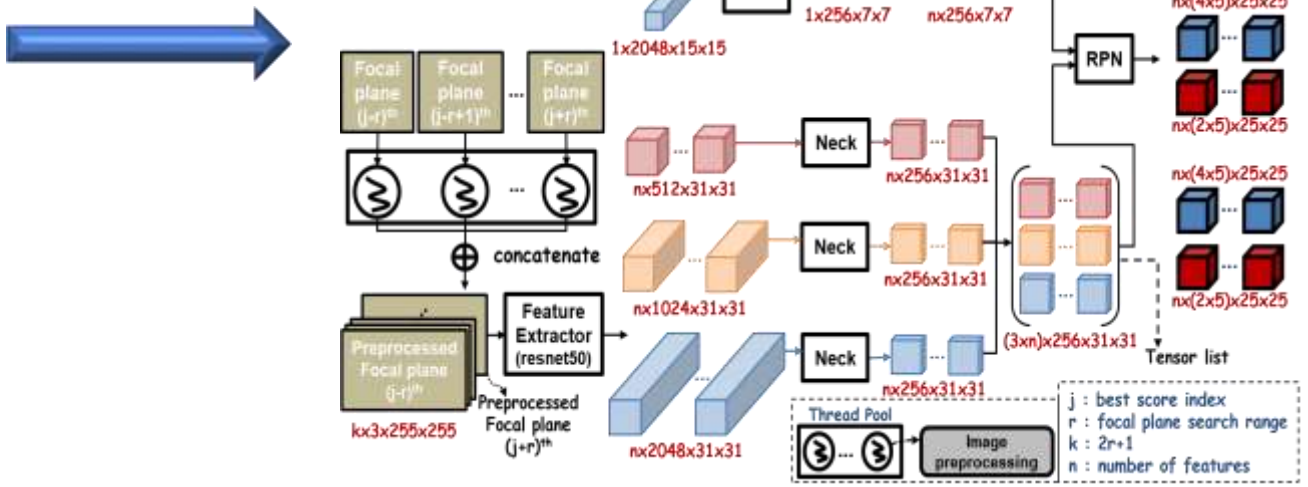
✓ 본 연구 개발의 최종 목표는 CPU 및 GPU 구조에 기반하여 병렬화 및 최적화된 **객체 추적 알고리즘**을 구현함으로써 **플렌옵틱 영상 시퀀스 입력에 대한 고속/고정밀의 단일 및 다중 객체 추적이 가능한 기술을 개발**하기 위함

- **with Hansung University & ETRI**
- **Mar. 2022 ~ Nov. 2022**

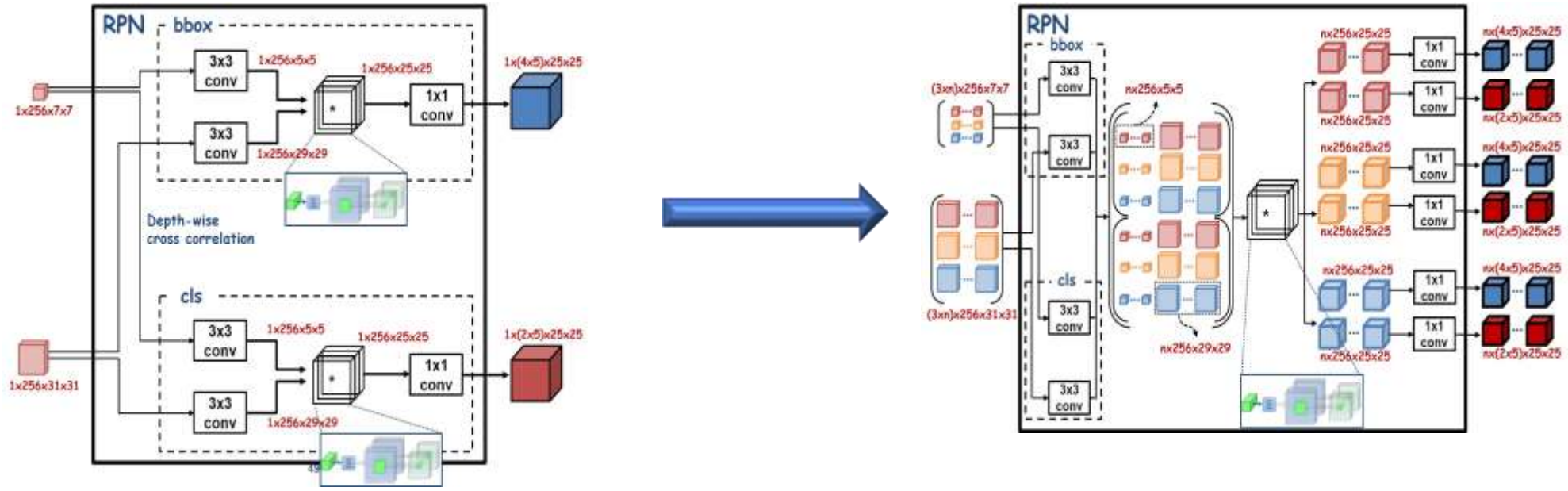
- **GOAL**
  - Python으로 구현된 Siamrpn++의 플렌옵틱 영상 다중 객체 추적의 속도 향상 및 최적화 (4sec/frame)

- **Contributions**
  - 이미지 전처리 과정 멀티 스레드화
    - ✓ 하나의 프로세스 내에서 여러 개의 이미지 전처리 스레드를 생성하여 CPU에서 동시에 여러 포컬플레인에 대한 이미지 전처리 진행





- **Contributions**
  - 포컬플레인을 batch 단위로 입력 받음
    - ✓ Resnet-50을 통한 feature 추출이 batch 크기에 비례하여 횟수가 감소됨
    - ✓ RPN 당 Depth-wise cross correlation 연산 회수를 2번에서 1번으로 줄임



- **Result**
  - 추적 속도가 19.6% 감소하여 4sec/frame을 충족하는 3.41sec/frame 달성

실행 version	sec/frame
Python version	4.24
Solution version	3.41

Paper 01.

Time-Constrained Adversarial Defense in IoT Edge Devices through Kernel Tensor Decomposition and Multi-DNN Scheduling

About paper

✓ 본 논문은 **비 선제적 장치인 임베디드 GPU**에서 여러 인공지능 어플리케이션이 동시에 실행되고 있을 때 **적대적 예제 복원 작업이 빠르고 우선적으로 실행**될 수 있도록 하는 **GPU 스케줄링 프레임워크**를 제안함.

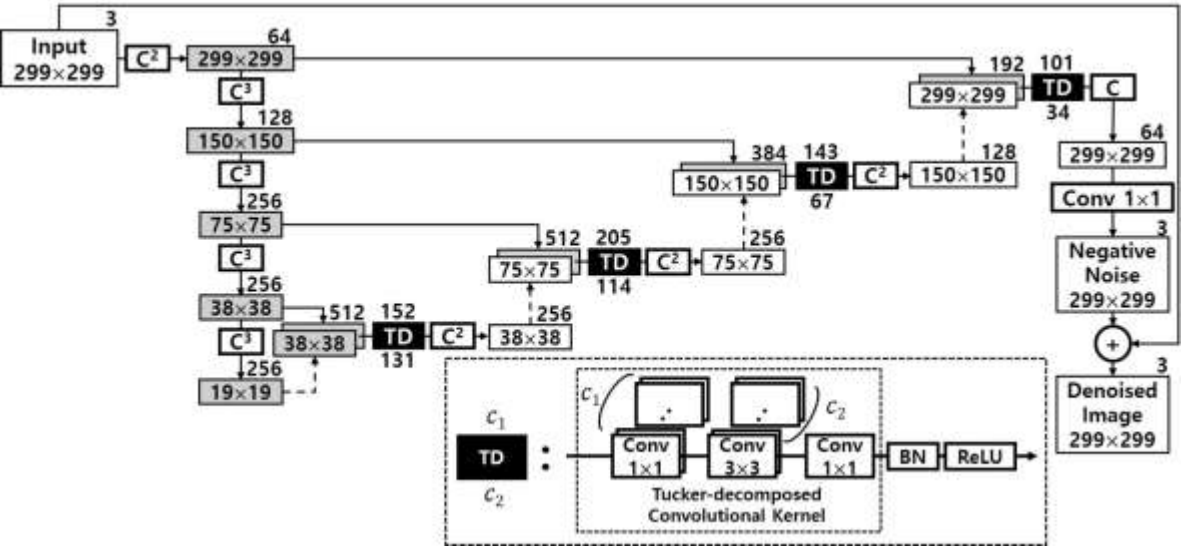
✓ github : https://github.com/jsun94/eDenoiser

- **국외 SCIE (MDPI Sensors)**
- **게재일 : 2022.08.07**

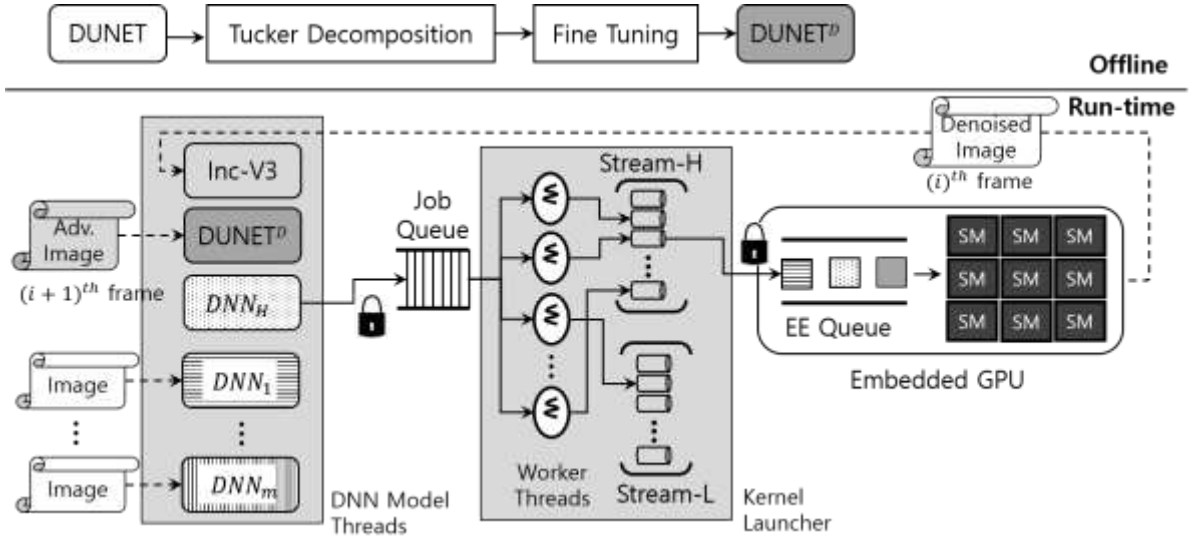
Paper 01. Time-Constrained Adversarial Defense in IoT Edge Devices through Kernel Tensor Decomposition and Multi-DNN Scheduling

- **GOAL**
  - 본 논문은 임베디드 시스템(Jetson AGX Xavier)에서 여러 DNN이 하나의 GPU에서 실행 중일 때 적대적 예제 복원을 빠르고 우선적으로 실행하고자 함

- **Contributions**
  - 추론 시간이 오래 걸리는 DUNET에 경량화를 진행
    - ✓ Tucker Decomposition을 4곳의 Convolution Kernel에 적용
  - 한 개의 임베디드 GPU에서 여러 DNN이 동시에 실행될 때 적대적 예제 복원이 우선적으로 실행되는 GPU Scheduling Framework 제안



Tucker Decomposed DUNET

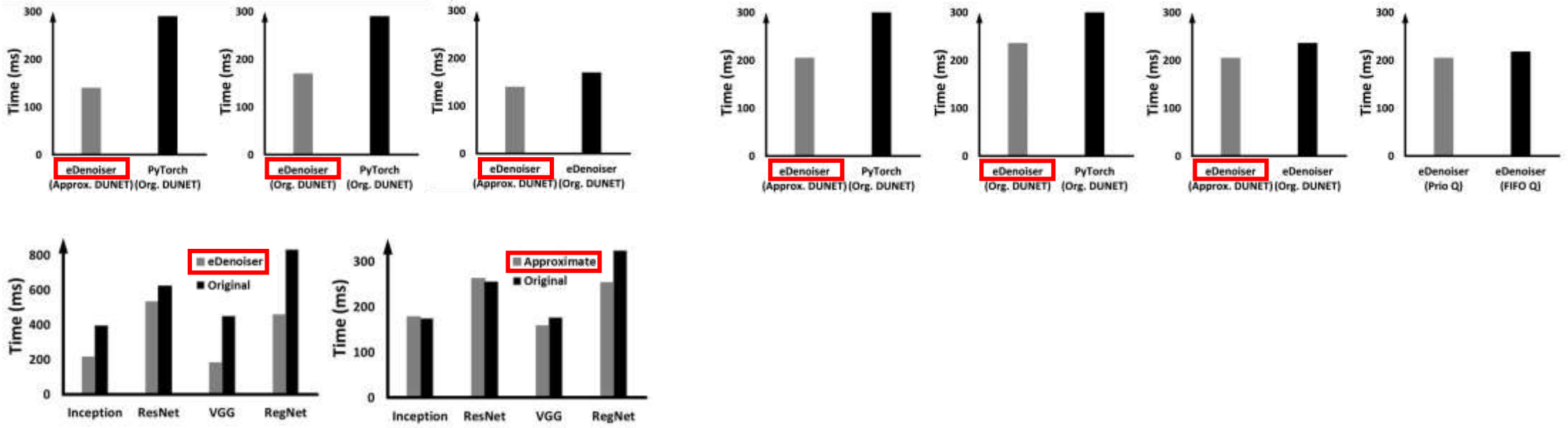


Workflow of proposed GPU Scheduling Framework

- **Result**
  - Tucker Decomposed DUNET의 정확도 감소율이 미미함 (최대 1.78%)

	Result in [8]	Org. DUNET	Approx. DUNET
Clean-image-test-set	76.2%	76.53%	76.38%
White-box-test-set	75.2%	72.37%	70.59%
Black-box-test-set	75.1%	74.86%	74.45%

  - 여러 실험 환경에서 Tucker Decomposed DUNET의 효능, Scheduler의 세부 기능 효능 및 전체 효능을 확인



  - Tucker Decomposition 및 Scheduler 적용 전 대비 적대적 예제 복원 속도가 최대 51.72% 향상됨

Paper 02.

소프트웨어 기반 임베디드 시스템용 적대적 공격 검출 시스템

About paper

✓ 본 논문은 성능은 좋지만 메모리 사용량이 크고 수행 시간이 오래 걸리는 적대적 공격 탐지 기법인 **NIC**(Neural Network Invariant Checking)를 임베디드 시스템에서 target DNN과 동시에 실행할 수 있도록 개량한 **소프트웨어 기반 시스템**을 제안함.

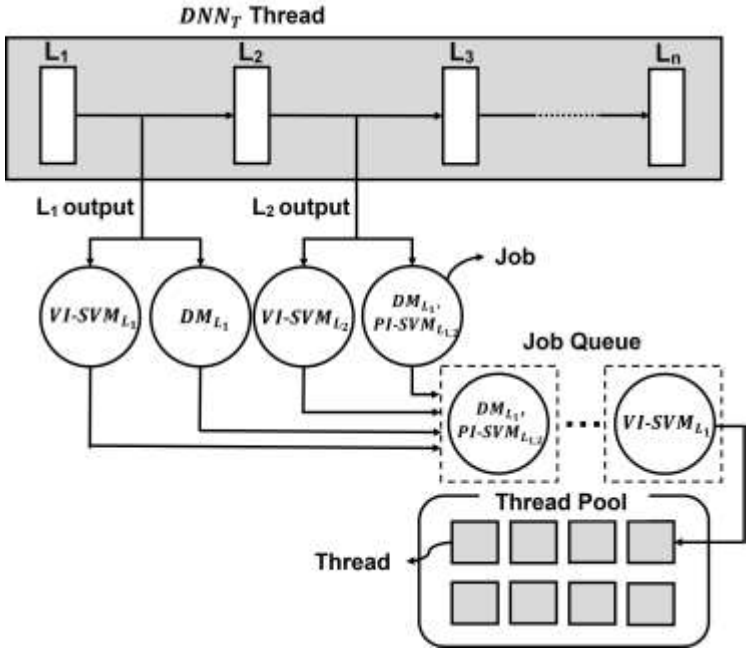
✓ github : https://github.com/jsun94/Embedded_NIC

- **국내 SCIE (대한전자공학회)**
- **게재일 : 2022.07.25**

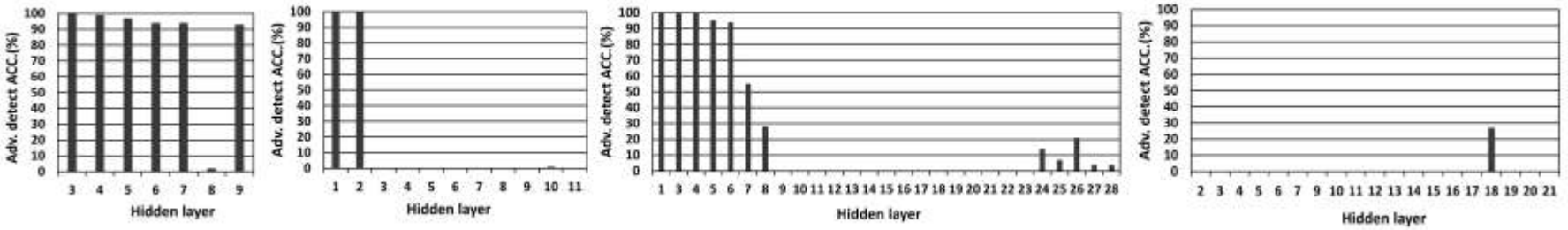
소프트웨어 기반 임베디드 시스템용 적대적 공격 검출 시스템

- **GOAL**
  - 본 논문은 임베디드 시스템(Jetson AGX Xavier)에서 하드웨어 변경 없이 NIC와 target DNN을 동시에 실행하여 두 개의 수행 종료 시간 차이를 최소화하고 메모리 사용량을 최소화 하고자 함

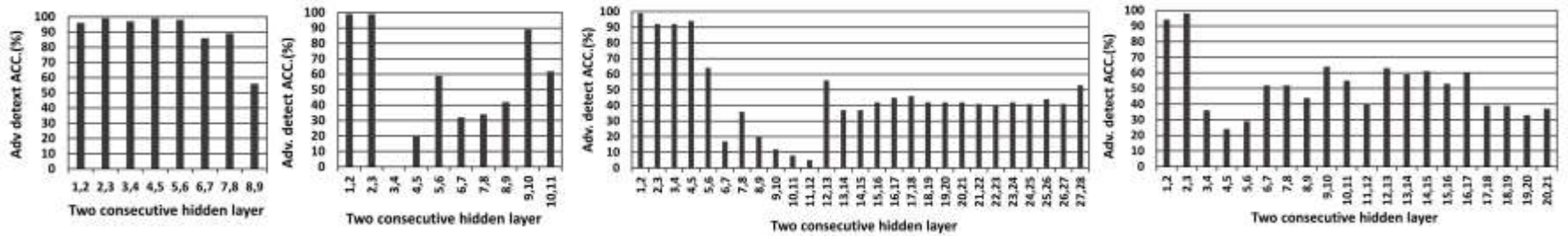
- **Contributions**
  - Multi Thread 기반 시스템을 설계하여 GPU와 CPU의 동시 사용량을 최대화하여 NIC와 target DNN의 수행 시간 차이를 좁힘
  - target DNN의 특정 layer에서만 공격 탐지를 진행하여 target DNN별 메모리 사용량을 최소화함



Workflow of proposed system

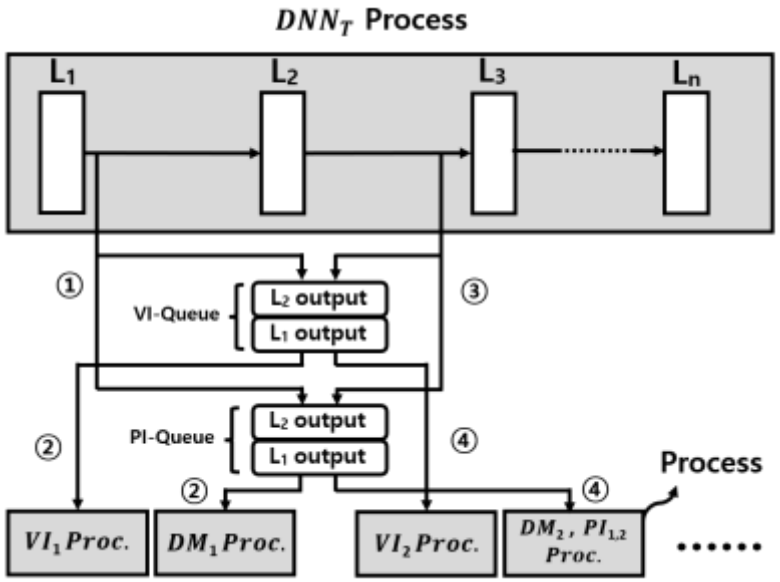


VI violation detection rate of adversarial examples in each hidden layer of the target DNN



PI violation detection rate of adversarial examples in each hidden layer of the target DNN

- **Result**
  - 제안한 시스템의 성능을 확인하기 위해 기존 멀티 프로세스 환경을 직접 구현



✓ t_{diff} : target DNN 추론 완료 시간 – 공격 탐지 종료 시간

  - 제안한 시스템 적용 전 대비 실행 시간 최대 95.2%, t_{diff} 최대 99.6%, 메모리 사용량 최대 83.9% 감소