SNN 기반 GPS Spoofing 탐지 모델 개발 및 클라우드 웹서비스 배포

	전공	이름
	정보통신공학과	박재현
	컴퓨터공학과	박지호

목차

1. 서론

프로젝트 배경: 초연결 모빌리티 시대의 도래와 보안 위협의 진화

Connected Car 생태계의 확산

- **달리는 스마트폰:** 단순 이동 수단에서 데이터 플랫폼으로 진화
- **V2X 확장:** 신호등, 타 차량, 클라우드와 실시간 소통
- **Risk:** 외부 네트워크 연결 → 공격 표면 급증

자율주행의 핵심, GPS 의존성 심화

- **자율주행 고도화:** cm 단위 위치 파악을 위한 필수 위치 센서
- **절대적 의존성:** 경로 설정 및 V2X 시간 동기화의 기준점
- **Criticality:** GPS 마비 시 자율주행 기능 불능

민간용 GPS의 구조적 취약점

- **보안 부재:** 군용과 달리 암호화/인증 없는 **개방형 신호**
- **쉬운 공격:** 저가형 SDR 장비로 위조 신호 생성 가능
- **Impact:** 실제보다 강한 신호로 **차량 제어권 탈취 위험**

문제 정의: GPS Spoofing 공격이 초래하는 치명적 위험

Jamming
신호 차단 → 수신 불능 → System Fail

VS

Spoofing
가짜 신호 주입 → 위치/시간 기만 → Receiver Hijacking

공격자는 차량의 실제 위치를 은밀하게 조작하여 운전자나 시스템이 인지하지 못하는 사이에 목표 지점으로 유인할 수 있다.

시나리오 1: 타겟 납치

- 자율주행 트럭/VIP 차량 타겟
- 인적이 드문 곳으로 유인
- 물류 탈취 및 인질극 가능성

시나리오 2: 대형 참사

- 고속 주행 중 급정거/급조향 유발
- 반대 차선/절벽으로 위치 인식
- 치명적 연쇄 추돌 사고

시나리오 3: 인프라 마비

- 주요 교차로/터널 위치 교란
- 다수 차량 동시 제어 불능
- 도시 교통망 마비 초래

GPS Spoofing 탐지의 필요성

Safety Assurance (안전 보장)

- **실시간 탐지:** 잘못된 주행 판단을 내리기 전에 찰나의 순간 공격을 인지
- **사고 미연 방지:** 승객과 보행자의 생명 보호를 위한 최우선 선결 과제

System Reliability (시스템 신뢰성)

- **무결성 감시:** GPS 신호 오염 즉시 감지하여 시스템 마비 방지
- **제어권 이양:** 공격 탐지 시, 즉각적으로 대체 센서나 안전 모드로 전환하는 신호탄 역할

Proactive Response (선제적 대응)

- **위협의 비례 증가:** 자율주행 보급 확대에 따라 공격 시도 역시 급증
- **방어 체계 구축기여:** 진화하는 해킹 기술에 대응하는 필수적인 보안 인프라

2. 관련 연구

기존 탐지 기술의 현황: 신호 처리 및 머신러닝

구분	신호 처리 기반 방법	머신러닝 기반 방법
핵심 원리	수신된 GPS 신호 자체의 물리적 특성이나 파형을 분석하여 스푸핑 공격을 식별	데이터 분석 및 인공지능 알고리즘을 활용해 정상 데이터와 공격 데이터를 구분
주요 한계	• **개별 센서 중심:** 차량 전체 시스템 고려 부족 • **시뮬레이션 의존:** Matlab 등 제한된 환경	• **데이터 한계:** 소규모/시뮬레이션 데이터셋 • **연산 효율성:** 자원 제약 환경 검증 부족
실제 주행 환경의 복잡성을 충분히 반영하지 못한다.		

물리 모델 기반 탐지의 진화와 한계

전통적 접근: 물리 모델 & EKF (Extended Kalman Filter)	
핵심 원리	차량 동역학 모델 + 센서 융합 (IMU + GPS) → 예측값과 측정값 편차 모니터링
주요 한계	복잡한 모델링 과정 **치명적 단점: 탐지 지연 약 23초**

개선된 접근: GPS-IDS (Hybrid Physics-based)	
핵심 원리	• 물리적 거동 모델 + 머신러닝 • 물리 모델에서 도출된 예측값과 실제 GPS 데이터 간의 상관관계를 시계열적 특징으로 추출 후 머신러닝 모델에 입력
EKF 대비 탐지 시간을 **약 56.5% 단축했으나**, **엣지장치에 대한 검증, 배포 방안 부족**	

현존 기술의 한계 및 향후 연구 방향

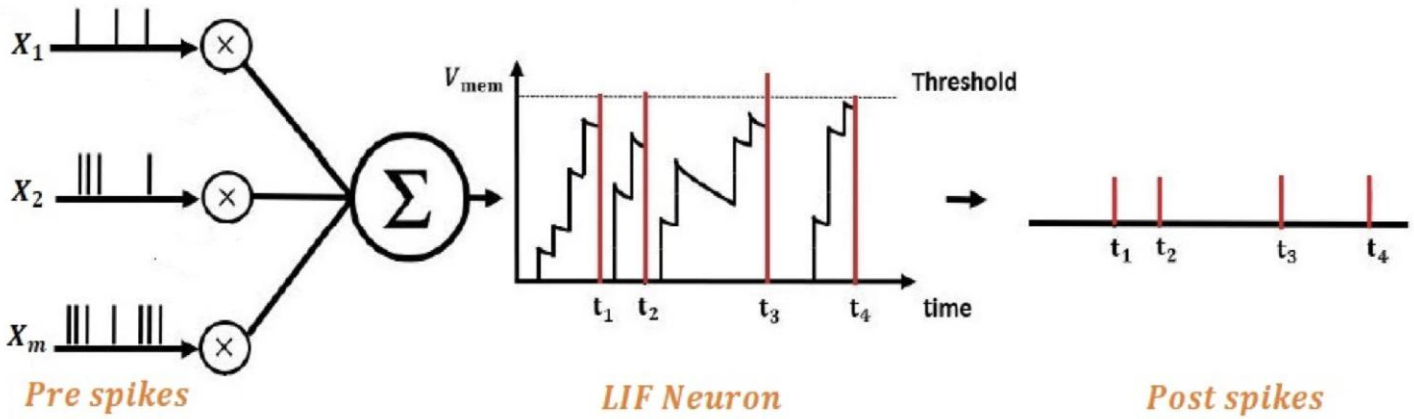
탐지 지연 (Latency Issue)	엣지 디바이스 효율성 (Efficiency)	지능형 공격 대응 (Generalization)
• GPS-IDS가 시간을 단축했으나 여전히 **지연** 존재 • 자율주행 환경에서 사고 방지를 위한 **초저지연 탐지** 대응 미흡	• 기존 연구는 고성능 PC 기반 검증 • 자원이 제한된 **엣지 디바이스 환경**에서의 실시간성 검증 부재	• **최신 공격 기법**에 대한 탐지 능력 확장 필요

실제 엣지 디바이스 환경에서 실시간으로 동작하며
지능형 공격 방어를 위한 경량화된 탐지 모델이 필요하다.

3. 제안 방법론

기반 기술: SNN (Spiking Neural Network)

딥러닝 모델의 높은 연산 비용을 해결하기 위해 SNN을 도입



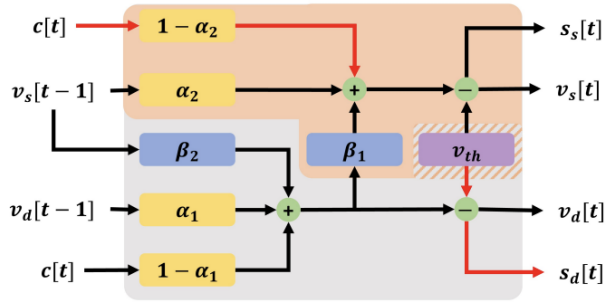
- **Event-driven Processing**
  데이터가 지속적으로 연산되는 기존 신경망과 달리 입력 신호가 Threshold를 넘는 시점에만 이산적인 스파이크를 발생
- **Silent Processing** (Neuromorphic Hardware 사용 시)
  데이터의 변화가 없거나 미미한 구간에서는 연산을 수행하지 않는 특성을 통해 불필요한 전력 소모를 획기적으로 절감

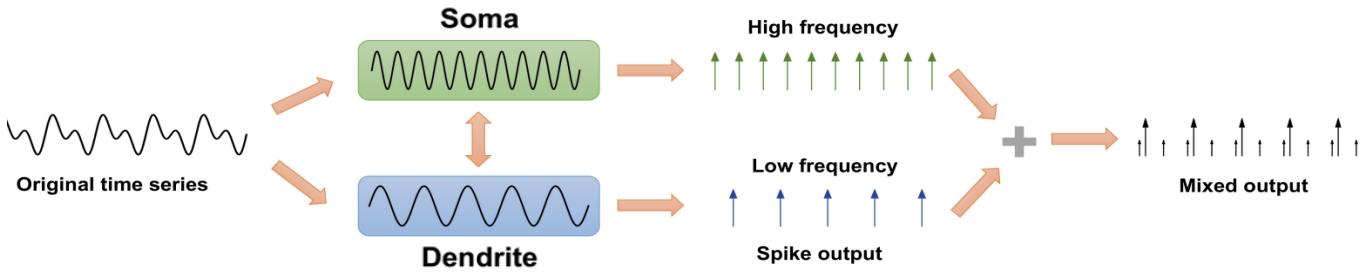
이론적으로 기존 ANN 시계열모델 대비 약 60~75%의 에너지 소비 감소 효과

https://link.springer.com/article/10.1007/s13748-024-00313-4/figures/3

핵심 뉴런 모델: TS-LIF (Temporal Segment LIF)

LIF 뉴런이 장기 의존성 포착에 취약하다는 단점을 보완하기 위해 TS-LIF 모델을 도입





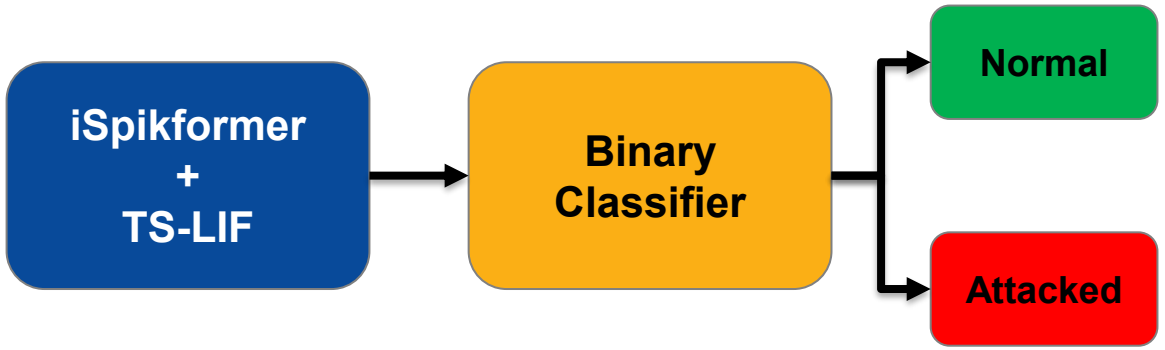
- **생물학적 모방:** 인간 신경 세포를 모사한 Dual-compartment 구조를 통해 시계열 데이터를 주파수 대역별로 분리
  - **수상돌기(Dendrite)**
    입력 신호의 저주파 성분을 필터링하여 장기적인 추세를 학습
  - **세포체(Soma)**
    고주파 성분을 감지하여 급격한 변동을 포착

장단기 패턴을 동시에 포착해 더 정확한 예측 가능

https://doi.org/10.48550/arXiv.2503.05108

전체 모델 아키텍처: TS-Former

TS-LIF을 연산 노드로 사용하는 TS-Former 모델을 구축하고 Binary Classification에 맞게 최적화



- **Backbone 재설계**
  SNN 기반 트랜스포머 구조인 iSpikformer를 베이스라인으로 채택하되 내부의 모든 스파이킹 뉴런을 TS-LIF로 전면 교체하여 시간적/주파수적 특징 추출 능력을 극대화
- **Binary Classification Head 결합**
  기존 iSpikformer의 Head를 변경해 입력된 GPS 시퀀스의 정상/공격 여부를 확률값으로 직접 출력
- **초경량화 설계**
  차량 내 임베디드 환경 탑재를 위해 모델의 전체 파라미터 수를 **약 29.3k 수준**으로 경량화

4. 시스템 아키텍처

팀원별 역할 및 프로젝트 진행 일정

■ 팀원별 역할

- **박재현:** 모델 구축 및 학습, 추론 서버 구축
- **박지호:** 데이터셋 분석 및 전처리, 웹 서버 구축

■ 프로젝트 진행 일정

Week	10월 5주차					11월 1주차					11월 2주차					11월 3주차				
요일	월	화	수	목	금	월	화	수	목	금	월	화	수	목	금	월	화	수	목	금
데이터셋 분석																				
데이터 전처리																				
모델 구축																				
모델 훈련 및 추론 실험																				
추론 서버 구축																				
웹 서버 구축																				
최종 프로젝트 검증																				

배포 전략: Cloud-Native 접근

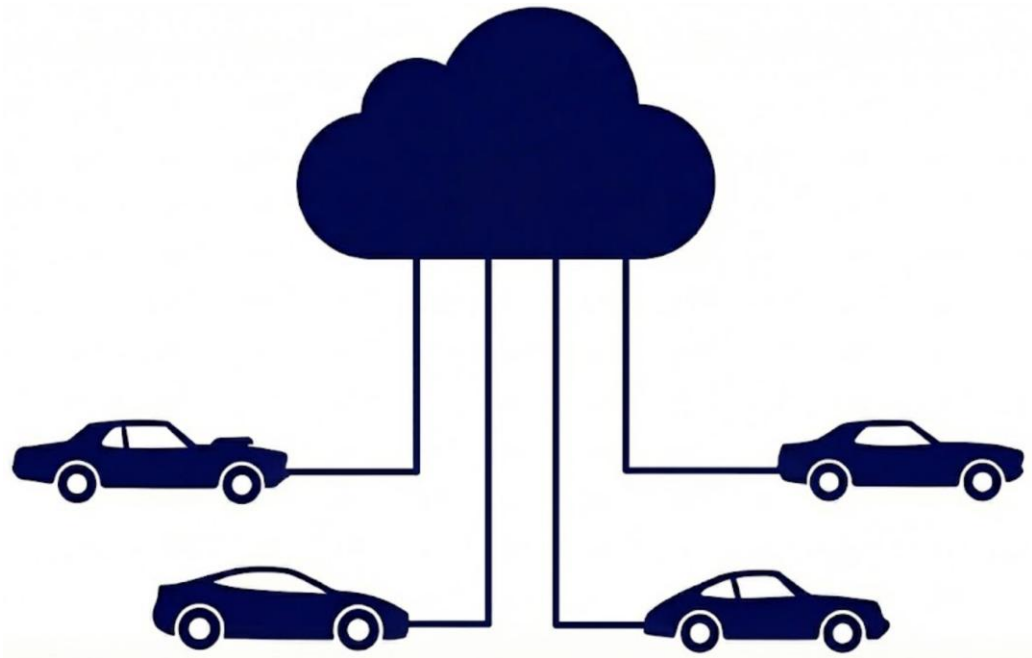
파편화된 자동차 OS 환경과 V2X 인프라의 물리적 제약을 고려하여
즉시 적용 가능한 클라우드 중심의 배포 전략을 수립

- **OS 비종속성 확보**

  차량의 제조사나 탑재된 OS 환경에 구애 받지 않고 표준화된 데이터 양식만 맞추면 Spoofing 여부 판별 가능

- **엣지 Porting을 위한 Testbed**

  클라우드 환경은 대규모 트래픽 처리 및 모델 성능 검증을 위한 테스트베드 역할을 수행하며 검증된 추론 모델은 향후 차량 내 엣지 디바이스로 경량화하여 이식 가능



MSA(Microservices Architecture) 기반 시스템 설계

보안성과 확장성을 고려하여 웹 서비스(Frontend)와 추론 엔진(Backend)을 물리적으로 분리된 두 개의 EC2 인스턴스로 구성

EC2 Instance 1
추론 전용 서버

• **역할:** 학습된 TS-Former 모델을 Flask 기반으로 상시 구동하여 실시간 분석을 수행

• **프로세스:** 전처리된 GPS 데이터를 수신 즉시 'Normal' 또는 'Attacked' 레이블로 반환

• **설계 의도:** 추론 로직의 완전한 독립을 통해 향후 Edge Device로의 이식성을 극대화

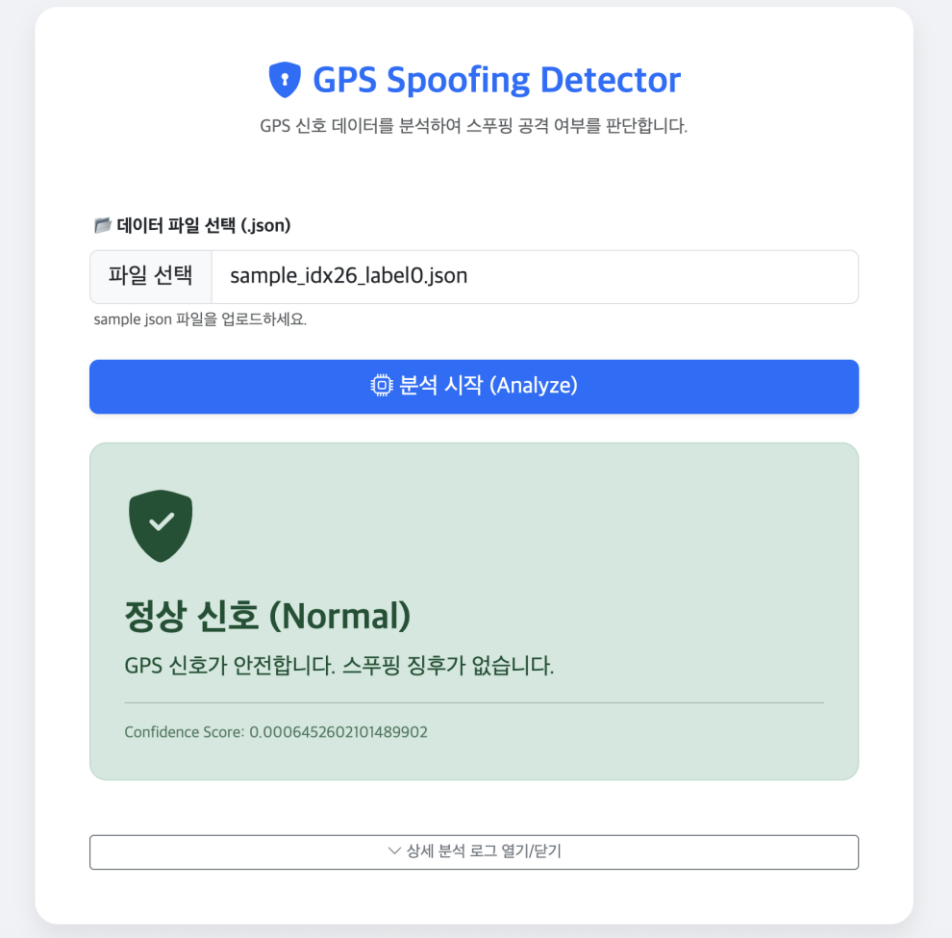
EC2 Instance 2
Web & Gateway

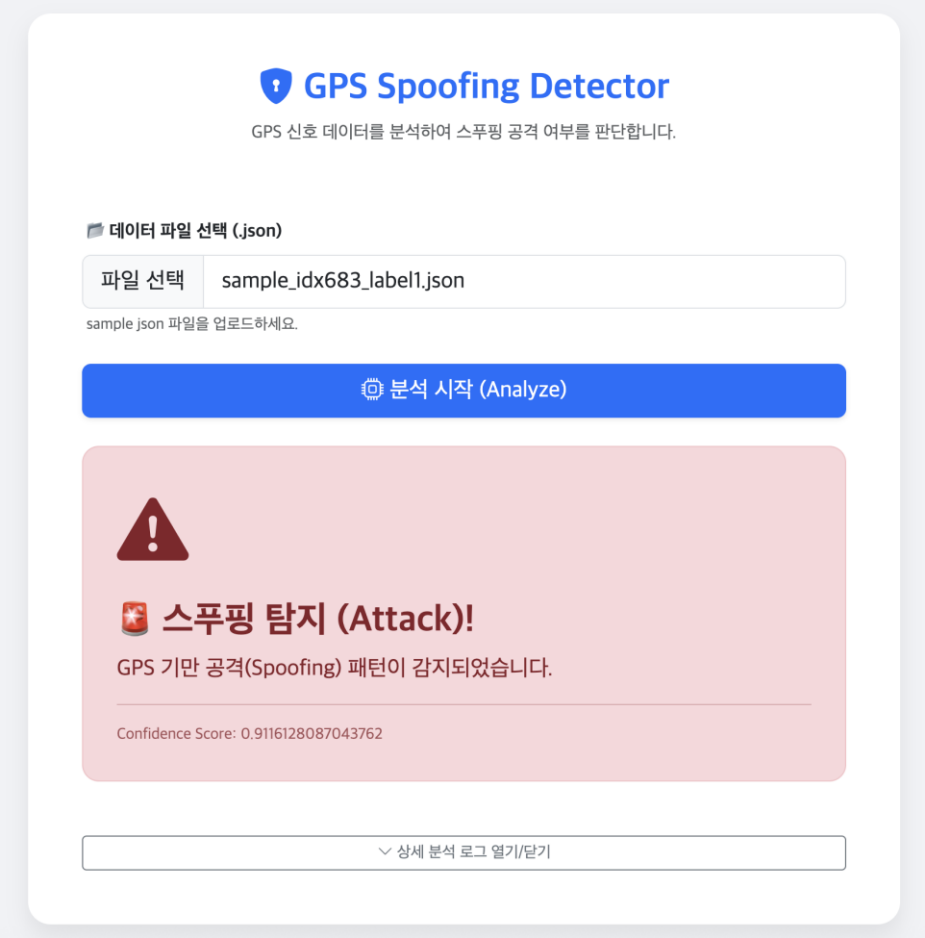
• **역할:** 사용자가 데이터를 입력하고 결과를 시각적으로 확인할 수 있는 웹 인터페이스 제공

• **Gateway 기능:** 외부 요청을 받아 추론 서버로 안전하게 중계하는 관문 역할을 수행

• **보안성:** 직접적인 모델 접근을 차단하여 시스템 안정성을 확보

프로젝트 시연 예시


GPS Spoofing Detector
GPS 신호 데이터를 분석하여 스푸핑 공격 여부를 판단합니다.
데이터 파일 선택 (.json)
파일 선택
sample_idx26_label0.json
sample json 파일을 업로드하세요.
분석 시작 (Analyze)
정상 신호 (Normal)
GPS 신호가 안전합니다. 스푸핑 징후가 없습니다.
Confidence Score: 0.0006452602101489902
상세 분석 로그 열기/닫기


GPS Spoofing Detector
GPS 신호 데이터를 분석하여 스푸핑 공격 여부를 판단합니다.
데이터 파일 선택 (.json)
파일 선택
sample_idx683_label1.json
sample json 파일을 업로드하세요.
분석 시작 (Analyze)
스푸핑 탐지 (Attack)!
GPS 기만 공격(Spoofing) 패턴이 감지되었습니다.
Confidence Score: 0.9116128087043762
상세 분석 로그 열기/닫기

5. 실험

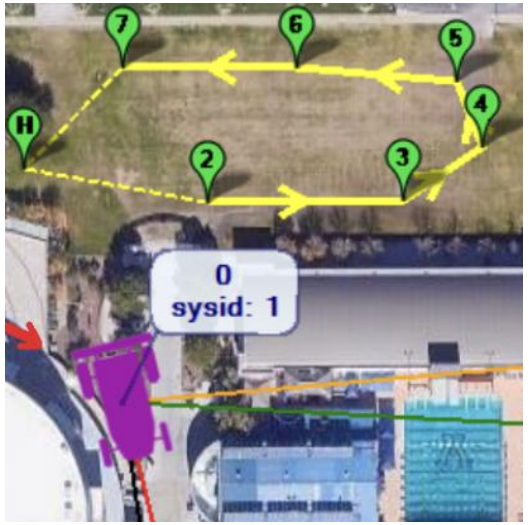
데이터셋 구성 및 전처리: AV-GPS Dataset

GPS-IDS에서 공개한 데이터셋으로 이 중에서 실제 주행 데이터셋을 실험에 활용

물리적 수집 환경

- **Platform:** GPS 수신기가 탑재된 1/10 Scale AVT
- **Attack:** HackRF One (SDR)을 이용해 실제 위성 신호와 구분하기 힘든 위조 GPS 신호를 송출

공격 시나리오



- **Drift Attack (직진 주행):** 직선 주행 중인 차량에 편향된 좌표를 주입
- **Turn Attack (회전 주행):** 곡선 구간에서 차량의 회전 반경이나 방향을 조작
- **Stop Attack (정차 상태):** 정차 중인 차량이 움직이는 것처럼 위조

데이터셋 전처리

① **결측치 처리:** 데이터 연속성을 위해 선형 보간을 적용

② **특징 선택:** IMU, 위성 수신 상태, 조향각 등 총 38개의 핵심 특징을 선별

③ **윈도우 생성:** 연속된 10초 묶음을 하나의 입력 단위로 구성

④ **데이터셋 분할:** train : val : test = 7 : 2 : 1

⑤ **데이터 정규화:** 모든 특징들을 0-1 사이의 값으로 변환

⑥ **학습 데이터 증강:** 과적합을 방지하기 위해 가우시안 노이즈를 무작위 주입

탐지 성능 비교

	GPS-IDS	Ours	Gap
F1	94.51%	**96.87%**	**▲ 2.36%p**
Accuracy	96.45%	**98.41%**	**▲ 1.96%p**
Precision	96.88%	**98.27%**	**▲ 1.39%p**
Recall	92.54%	**95.51%**	**▲ 2.97%p**
FPR	-	**0.58%**	-

*GPS-IDS: MLP 모델의 3가지 Case(I, II, III)에 대한 실험 결과 전체 평균
*Ours: Test Dataset에 대한 평가 결과

엣지 디바이스 효율성 평가

NVIDIA Jetson Orin Nano (8GB)를 사용해 엣지 환경에서의
실시간성 및 전력 효율성을 측정

추론 속도
• Mean latency/batch: **118.96 ms** • Mean latency/sample: **1.859 ms**

전력 및 에너지 소비 효율
• Avg / p90 / Max Power: **8.96 W / 10.23 W / 10.82 W** • Total Energy: **34.04 J (약 3.8초 구동 기준)**

6. 결론

결론 및 기대 효과

초연결 모빌리티 환경의 핵심 보안 위협인 GPS Spoofing을 탐지하기 위해 SNN 기반의 고효율·고성능 탐지 시스템을 구현

실시간 보안 서비스
• 인터넷에 연결된 차량의 GPS Spoofing 실시간 탐지 • 높은 정확도와 빠른 응답 속도로 신뢰성 확보 • API 제공으로 기존 차량 시스템과의 통합 용이
엣지 컴퓨팅 적용 가능성
• SNN의 전력 효율성으로 차량 내 온보드 배포 가능 • 클라우드-엣지 하이브리드 아키텍처 구현 가능 • 네트워크 지연 없는 즉각적인 탐지
안정성 향상
• 차량 Navigation 시스템의 보안 강화 • GPS 기반 ECU 오작동 방지 • 운전자 및 보행자 안전 확보

자율주행차 상용화 가속
• GPS 보안 문제 해결로 자율주행 기술 신뢰성 향상 • 안전한 자율주행 환경 조성
커넥티드 카 생태계 보안
• GPS 기반 서비스(내비게이션, 차량 추적, 긴급 구조 등)의 안전성 확보 • 차량 사이버 보안 표준 수립에 기여
범용적 적용
• 차량뿐 아니라 드론, UAS, 로봇 등 GPS 기반 시스템 전반에 적용 가능 • 국방, 물류, 공공안전 분야로 확장 가능

소감

박재현	커넥티드 카의 중요성에 대해서 생각해 볼 수 있었고, 보안적인 측면에 대한 연구가 더 많이 이루어져야겠다는 생각이 들었다.
박지호	커넥티드 카가 우리 삶에 어떤 편의를 제공하는지, 어떤 위험이 도사리고 있는지, 그리고 이러한 위험에 어떻게 대비해야 할지 생각해 보는 계기가 되어 좋았다.

감사합니다.