Journal of KIIT. Vol. 23, No. 10, pp. 97-108, Oct. 31, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.10.97

LSTM 기반 자율주행 실시간 GPS 스푸핑 이상 탐지 시스템

강태훈*, 최선오**

Real-Time GPS Spoofing Anomaly Detection System for Autonomous Driving based on LSTM

Taehun Kang*, Sunoh Choi**

요 약

본 연구는 자율주행 차량이 의존하는 GPS 신호가 외부 공격에 의해 조작될 수 있다는 보안 취약점에 주목하여 GPS 스푸핑 공격을 실시간으로 탐지할 수 있는 이상 탐지 시스템을 제안한다. 제안된 시스템은 스마트폰의 GPS 수신기를 통해 수집된 GPS 데이터를 서버로 전송하고 LSTM 기반 시계열 예측 모델을 활용하여 정상 GPS 데이터 흐름을 학습하고 실시간으로 수신되는 GPS 데이터와의 예측 오차를 분석하여 이상 탐지를 수행한다. 이상 판단에는 MAE, MA, AS를 결합한 다중 지표 기반 기준과 환경 변화에 따라 조절되는 Dynamic Threshold를 활용하여 신뢰성을 높였다. 모델 성능 평가는 정적 로그 데이터를 활용한 1차 평가와 실시간 데이터를 기반으로 한 2차 평가로 나누어 수행하였으며 중요한 2차 평가에서 정확도 98.69%의 우수한 성능을 기록하였다.

Abstract

This study addresses the security vulnerability that GPS signals, which autonomous vehicles rely on, can be manipulated by external attacks, and proposes an anomaly detection system capable of real-time detection of GPS spoofing attacks. The proposed system transmits GPS data collected via a smartphone's GPS receiver to a server and utilizes an LSTM-based time series prediction model to learn the patterns of normal GPS data flow. By analyzing the prediction errors between the model's forecast and the real-time GPS data, the system detects anomalies. For improved reliability, the anomaly determination incorporates a multi-metric approach that combines MAE, MA, and AS, along with a Dynamic Threshold that adapts to changing environmental conditions. Model performance was evaluated in two phases: an initial assessment using static log data and a second evaluation based on real-time data. The system achieved outstanding performance, with an accuracy of 98.69%.

Keywords

GPS spoofing, anomaly detection, HackRF One, autonomous vehicles, real-time detection, LSTM

* 전북대학교 소프트웨어공학과 학사과정
- ORCID: https://orcid.org/0009-0002-4244-581X
** 전북대학교 소프트웨어공학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-0654-7109

· Received: Jul. 31, 2025, Revised: Aug. 25, 2025, Accepted: Aug. 28, 2025

· Corresponding Author: Sunoh Choi
Dept. of Software Engineering Jeonbuk National University Korea
Tel.: +82-63-270-4784, Email: suno7@jbnu.ac.kr

Ⅰ. 서 론

최근 자율주행차(Autonomous vehicle)의 보급 확대와 더불어, 다양한 차량 내 센서와 외부 인프라가 주행에 적극 활용되고 있다. 이 중에서도 GPS(Global Positioning System)는 차량의 현재 위치를 판단하고 경로를 설정하며, 주행 속력과 방향을 제어하는 데 필수적인 역할을 수행한다. 특히 주행 중 끊임없이 변화하는 위치 정보를 정확히 인식하고 예측하는 것은 자율주행 알고리즘의 핵심 기반이며, 이로 인해 GPS 신호의 신뢰성과 무결성 확보는 안전 주행의 중요한 전제가 된다.

그러나 민간용 GPS는 암호화되지 않은 개방형 신호로 구성되어 있으며, 이로 인해 외부에서 조작된 위성 신호를 수신기에 전달하는 GPS 스푸핑(GPS spoofing) 공격이 비교적 쉽게 수행될 수 있는 구조적 한계를 지닌다. GPS 스푸핑 공격은 합법적인 위성 신호보다 강한 신호를 수신기에 보내어 GPS 수신기의 위치를 공격자가 의도한 가짜 위치로 동기화시키는 방식으로 작동하며, 일정 수준 이상의 정밀한 동기화 및 위변조가 가능할 경우, 수신기는 실제와 다른 위치를 인식하게 된다. 이러한 GPS의 보안 취약점은 단순히 차량의 위치정보를 혼란스럽게 만드는 수준을 넘어서 주행 경로 자체를 왜곡시켜 사고나 인명 피해로 이어질 수 있는 가능성이 존재한다.

실제로 Dasgupta et al.은 자율주행 차량을 대상으로 한 Slow Drift GPS 스푸핑 공격을 실험적으로 수행하여, 현실적인 주행 환경에서의 보안 위협을 실증하였다[1]. 이들은 공격 차량이 피해 차량을 일정 거리 내에서 따라가면서, 동일한 GPS 위성 신호를 수신한 후 사전에 정의한 스푸핑 경로에 따라 위조된 의사거리(Pseudorange) 값을 생성하고 이를 HackRF One 장비를 통해 송출함으로써, 피해 차량의 GPS 수신기가 점진적으로 잘못된 위치를 인식하도록 하였다. 이 과정은 기존 GPS 신호와 동일한 위성 ID 및 코드 구조를 유지하되 의사거리(Pseudorange) 값을 아주 조금씩 변화시키는 방식으로 이루어지며, 수신기는 공격 신호를 합법적인 신호로 판단하고 이를 그대로 반영하게 된다. 이러한 방식은 수신기 내부의 일관성 검사를 통과하면서도 위치를 점진적으로 왜곡시킬 수 있기 때문에, 운전자나 자율주행 시스템이 이상을 감지하기 어렵다.

실험은 실제 도시 환경에서 주행하는 차량을 대상으로 수행되었으며, 공격자는 피해 차량이 교차로에서 좌회전하는 시점에 맞추어 경로를 우회 방향으로 자연스럽게 변경하도록 스푸핑 경로를 설계하였다. 공격자는 수신기의 위치 인식을 아주 서서히 변화시켜, 시스템이 이를 정상 주행으로 받아들이게 만들었고, 이러한 점진적 경로 편향(Slow drift) 방식은 탐지를 회피하면서도 차량의 최종 경로를 완전히 다른 방향으로 유도하는 데 성공하였다. 공격이 완료된 이후 스푸핑된 GPS 경로와 실제 주행 경로를 비교한 결과를 보면, 전체 경로의 차이는 명확하게 드러났지만 실시간 운행 중에는 수신기나 운전자가 이를 감지하지 못하였다. 실험 데이터 분석에서는 두 경로 간 상관관계인 R^2 값이 0.99~1.0으로 매우 높게 나타났으며, 이는 GPS 수신기가 스푸핑된 경로를 정상적인 위치 정보로 신뢰하고 받아들였음을 의미한다. 연구진은 이러한 실험을 통해 점진적 스푸핑 방식이 자율주행 차량의 판단 알고리즘과 센서 융합 구조를 모두 우회할 수 있다는 점을 실증적으로 입증하였다.

또한, Tesla Model 3 차량의 자율주행 보조 시스템인 Navigate on Autopilot 기능은 HackRF One 기반 GPS 스푸핑 공격 실험에서 명백한 오작동 반응을 보인 바 있다. 해당 실험에서는 공격자가 SDR 장비를 통해 조작된 GPS 신호를 송출하자, 차량은 실제 위치와 무관한 잘못된 도로 정보를 인식하였고, 이로 인해 고속도로 진입로에서의 우선순위 판단에 실패하거나, 잘못된 속도 제한을 적용하여 주행 안정성을 심각하게 해칠 수 있는 상황이 발생하였다. 이는 상용 자율주행 차량이 실제 환경에서 스푸핑 공격에 의해 쉽게 교란될 수 있으며, GPS 의존성이 높은 시스템일수록 보안적 위협에 취약하다는 사실을 실증적으로 보여준다[2]. 이처럼 자율주행차가 외부 GPS 정보에 강하게 의존하는 구조하에서 GPS 스푸핑 공격에 대응하기 위해서는, 고가의 센서 융합 장비나 외부 인프라에 의존하지 않으면서도, 실시간으로 위치 이상을 탐지할 수 있는 독

립적인 이상 탐지 기술이 요구된다.

본 연구에서는 이를 해결하기 위한 접근으로, 단일 LSTM(Long Short-Term Memory) 기반 시계열 예측 모델을 이용한 GPS 이상 탐지 방식을 제안한다. 제안된 방법은 정상적인 GPS 시계열 데이터를 기반으로 향후 위치를 예측하고, 이를 실제 수신된 GPS 좌표와 비교함으로써 비정상적인 움직임을 판단한다. 예측된 결과와 실제 GPS 값 간의 평균 절대 오차(MAE, Mean Absolute Error), 이동 평균(MA, Moving Average), 위도/경도 차이, 고도 차이, 3D 이동 거리 차이 등의 요소를 종합적으로 고려하여 이상 여부를 판별하며, GPS 스푸핑이 지속되는 상황과 급변하는 위치 변화도 동시에 감지할 수 있도록 다중 기준 기반 판단 로직을 설계하였다.

본 연구에서는 실제 차량에 탑승한 상태에서 스마트폰의 앱을 통해 GPS 데이터를 수집하고, 서버로 수집된 GPS 데이터를 전송한다. GPS 데이터는 위도, 경도, 고도, 속력, 시간을 포함하며 GPS 데이터는 스마트폰의 GPS 수신기 모듈을 통해 수집된다. 그 후 별도의 SDR 장비인 HackRF One[3]을 사용하여 GPS 스푸핑 공격 시나리오를 구성하고 수행함으로써, 실제 자율주행차의 상황과 비슷하게 실험을 설계하고, 해당 상황에서의 GPS 스푸핑에 대한 이상 탐지 성능을 실험적으로 검증하였다. 실험 결과, 제안된 이상 탐지 모델은 Accuracy 98.69%, Precision 97.65%, Recall 98.96%, F1-score 98.27%, FPR 1.46%를 기록하였다.

본 연구의 주요 기여는 다음과 같다. 첫째, 스마트폰의 GPS 수신 모듈을 활용하여 실제 차량 주행 환경에서 GPS 데이터를 실시간으로 수집하고, HackRF One 장치를 이용하여 GPS 스푸핑 공격을 수행함으로써, 자율주행 차량 환경에 근접한 현실적인 실험 시나리오를 구성하였다. 둘째, 단일 LSTM(Long Short-Term Memory) 기반의 시계열 예측 모델을 적용하여 모델 구조의 복잡성을 낮추는 동시에, 다중 지표 기반 이상 탐지 방식을 설계함으로써 실시간 탐지 성능을 강화하였다. 셋째, 정적 로그 데이터를 활용한 오프라인 평가와 차량 운행 중 실시간 GPS 데이터를 활용한 실시간 평가로 구성된 이중 검증 절차를 통해, 모델의 이상 탐지 정확도뿐만 아니라 실시간 대응 가능성까지 실험적으로 입증하였다. 넷째, GPS 환경에서 발생할 수 있는 노이즈나 일시적 수신 오류로 인한 오탐을 최소화하고 지속적 이상 탐지에 신뢰성을 부여하는 방향으로 판단 기준을 정교화함으로써, 향후 자율주행 시스템 등의 실제 환경 적용 가능성에 대한 기초 연구로서의 의의를 가진다.

본 논문의 구성은 다음과 같다. 2장에서는 GPS 스푸핑 탐지와 관련된 기존 연구를 분석하고, 본 연구와의 차별성을 설명한다. 3장에서는 GPS 스푸핑의 개념과 공격 방식, 그리고 실험에 사용된 HackRF One 장비에 대해 소개한다. 4장에서는 본 연구에서 제안하는 이상 탐지 시스템의 전체 구조와 이상 판단 방법에 대해 상세히 설명하며, 5장에서는 수집된 실험 데이터를 기반으로 모델의 성능을 두 번에 걸쳐 평가한다. 마지막으로 6장에서는 본 연구의 결론을 정리하고 향후 연구 방향을 제시한다.

II. 관련 연구

2.1 ML 기반 GPS 이상 탐지 기법

GPS 스푸핑은 위성 신호를 위조하여 수신기의 위치 인식을 왜곡시키는 공격으로, 자율주행 차량에 매우 치명적인 보안 위협이 된다. 이에 따라, GPS 신호의 시간적 패턴을 분석하여 이상을 탐지하는 기계학습(ML, Machine Learning) 기반 접근이 활발히 연구되고 있다. 그중에서도 LSTM(Long Short-Term Memory) 구조는 시계열 데이터를 다룰 때 장기적인 의존성과 패턴을 효과적으로 학습할 수 있어, GPS 데이터 기반 이상 탐지에 적합하다는 평가를 받고 있다.

D. Kiruthika and G. Ananthi[4]는 GPS 스푸핑 탐지를 위해 AHLSTM(Attention-enabled Hierarchical LSTM) 모델을 제안하였다. 해당 모델은 LSTM Autoencoder 구조에 계층적 Attention 메커니즘을 결합하여, 시계열 내 핵심 위치 정보를 강조하고 다양한 시간 단위의 이상을 효과적으로 탐지한다. 이 모델은 실험 결과 Accuracy 0.9926, F1-score 0.9723을 기록하며 기존 LSTM-AE 대비 우수한 성능을 보였다.

B. Wang et al.[5]은 자율주행 차량의 경로 데이터를 기반으로 LSTM Autoencoder와 Gaussian Mixture Model(GMM)을 결합한 이상 탐지 구조(LAGMM)를 제안하였다. 이 모델은 LSTM을 이용해 정상 시계열 패턴을 학습하고, GMM을 통해 예측값과 실제 GPS 간의 차이를 확률적으로 평가하여 이상을 판단하였다. 이를 통해 단순 재구성 오차 기반보다 더 정밀한 탐지 기준을 제공하였으며 기존의 방식(DAGMM, Deep Autoencoding Gaussian Mixture Model)보다 Accuracy를 3%, Precision을 6.4% 향상한 LAGMM을 제안하였다.

M. M. Abrar et al.[6]은 GPS-IDS 프레임워크를 제안하며, 먼저 물리 기반 동적 자전거 모델(Dynamic bicycle model)과 GPS 내비게이션 모델을 통합한 Autonomous Vehicle Behavior Model을 정의한다. 이 모델로부터 14개의 시계열 특징을 추출한다. 이들 특징을 입력으로 하여 지도학습 기반 분류기(Random Forest, XGBoost, SVM, AdaBoost, Gradient Boosting, Decision Tree, Multi-Layer Perceptron)를 비교 검증한 결과, MLP(Multi-Layer Perceptron)가 실제 데이터에서 F1-score 94.4%, 시뮬레이션 데이터에서 97.1%를 기록하며 가장 우수한 성능을 보였다. 또한 실시간성 평가에서 MLP는 공격 발생 후 10초 만에 스푸핑을 탐지하여, 기존 EKF 기반 GPS/INS 검출(23초) 대비 약 56.5% 빠른 탐지 성능을 확인하였다. 이처럼 GPS-IDS는 복잡한 딥러닝 없이도 물리 모델과 ML 분류기의 결합만으로 높은 탐지 정확도와 실시간 대응 능력을 동시에 달성하였다.

K. Lee et al.[7]은 실제 국내 대학생의 라이프로그 기반 GPS 이동 경로 데이터(DSEM-Trajectory)를 활용하여 CNN, DNN, LSTM, Bi-LSTM, LSTM Autoencoder 등 5가지 딥러닝 모델의 이상치 탐지 성능을 비교 분석하였다. 실험 결과, LSTM Autoencoder 모델이 평균 F1-score 88.67%로 다른 모델에 비해 가장 우수한 성능을 보였다. 해당 논문에서는 이동 경로 데이터의 이상치를 점 이상치, 집단적 이상치, 상황적 이상치로 구분하여 정의하고, 지도 기반의 경로를 그리드화한 후 이를 딥러닝 모델에 학습시켜 기존 필터링이나 수동 검수만으로는 탐지하기 어려운 복잡한 이상 유형까지 딥러닝 기반 모델의 학습을 통해 효과적으로 탐지할 수 있음을 실증하였다. 특히 LSTM 기반인 LSTM Autoencoder는 정상 데이터만을 이용하는 비지도 학습 방식으로 사용자 경로의 복잡한 패턴 재구성을 기반으로 이상 탐지를 수행함으로써, 데이터셋의 품질 관리와 실제 데이터 기반의 지능형 이상 탐지 연구에서 그 의의를 가진다.

기존의 ML 기반 탐지 기법들(AHLSTM, LAGMM 등)은 일부 정확도 지표에서 우수한 성능을 보고한다. 그러나 자율주행 시스템에서는 정확도 - 지연 간 상충(Trade-off)이 존재하며, 약간의 정확도 향상을 위해 반응 지연이 커지는 선택은 실용적, 안전적 측면에서 바람직하지 않다. 본 연구의 단일 LSTM은 기존의 ML 기반 탐지 기법들 보다 우수한 성능을 달성하면서 구조적 단순성을 통해 실시간성과 경량성, 정확성의 균형을 제공한다.

한편, LAGMM은 샘플당 약 80 ms의 추론 지연을 보고하였고, AHLSTM은 추론 지연 수치를 미보고한 채 계산 효율성 향상을 향후 과제로 제시하였다. 이는 복잡한 모델의 실시간 적용 가능성 평가에 필요한 근거가 부족함을 시사한다.

반면, 단일 LSTM을 활용한 유사 과업에서 모델 추론 지연이 약 2 ms로 보고된 사례가 있어 단일 LSTM 구조의 저지연 잠재력을 뒷받침한다[8]. 결과적으로, 즉각적 반응이 필수적인 자율주행과 같은 데이터가 스트리밍 환경에서는 단일 LSTM 기반 구조가 효율적이고 실용적인 대안이 될 수 있다.

2.2 자율주행 차량 기반 GPS 스푸핑 실험

GPS 스푸핑 이상 탐지 모델의 실효성을 검증하기 위해서는 실시간성과 현실성을 갖춘 실험 환경에서의 평가가 필요하다. 특히 자율주행 차량은 GPS 신호에 대한 의존도가 높고, 실시간 판단이 중요한 특성을 가지므로, 실제 차량 실험 또는 실시간 시뮬레이션이나 실험을 통한 검증이 중요하다.

S. Dasgupta et al.[9]는 자율주행 차량의 GNSS, CAN, IMU 센서 데이터를 융합하여, LSTM 기반 시계열 예측 모델로 두 시점 간 이동 거리를 예측하고, 실제 GNSS 이동 거리와의 오차가 임계값을 초과할 때 스푸핑 공격을 탐지하는 방법을 제안하였

다. 이 방법은 공개된 정적 로그 데이터를 기반으로 한 오프라인 평가에 초점이 맞추어져 있으며, 이론상 실시간 적용 가능성을 보였으나, 실제 차량 주행 환경에서의 실시간 검증은 이루어지지 않았다.

이에 반해 본 연구는 스마트폰 GPS 수신 모듈을 통해 실시간으로 데이터를 수집하고, Flask 서버를 통해 이를 전송한 후, LSTM 기반 예측 모델을 이용해 실시간 이상 판단을 수행하는 구조를 구현하였다. 특히 모델은 실시간으로 계산된 MAE, MA, AS와 이동 거리 기반 지표를 결합하여 신속한 판단을 가능하게 한다. 또한 HackRF One SDR 장비를 통해 실제 GPS 스푸핑 신호를 생성, 송출하고, 이를 차량 내의 스마트폰에서 수신함으로써 실제 환경에서의 공격 시나리오를 정밀하게 재현하였다.

이는 정적 로그 데이터 기반의 모델 검증과 달리, 차량 운행 중 차량 내부의 스마트폰으로 수집되는 실시간 데이터를 바탕으로 한 이상 탐지 구조로서 현실적인 조건 하에서의 실시간 반응성과 검출 가능성을 중점적으로 검증하였다. 이러한 구조는 탐지 정확도뿐만 아니라 실시간 대응성, 현장 적용 가능성을 고려하고, 무엇보다 실시간 대응 능력과 실험적 신뢰성 측면에서 기존 연구들과의 실용적 차별성을 갖는다.

III. 배경지식

3.1 GPS 스푸핑

GPS 스푸핑(GPS spoofing)은 공격자가 위조된 GPS 신호를 전송하여 GPS 수신기의 위치 인식을 조작하는 공격 방식이다. GPS 수신기는 보통 신호 세기가 가장 강한 위성 신호를 신뢰하므로, 공격자가 의도적으로 생성한 위조 신호가 실제 신호보다 세기가 강할 경우 이를 실제 위성 신호로 오인하게 된다. 이로 인해 GPS 수신기의 위치 정보가 왜곡되며, 자율주행 시스템과 같은 위치 기반 의사결정 시스템에 심각한 영향을 초래할 수 있다.

GPS 스푸핑은 공격의 정밀도에 따라 다양한 유형으로 구분된다. 본 연구에서는 다음과 같은 두 가지 GPS 스푸핑 공격 시나리오를 설계하였다:

· 편향 이동 스푸핑: 실제 경로와 유사하지만 점진적으로 위치가 편향된 경로를 따라가도록 유도하는 GPS 스푸핑 공격 방식

· 이탈 경로 스푸핑: 실제 경로와 완전히 다른 경로로 차량을 유도하는 GPS 스푸핑 공격 방식

이러한 방식은 자율주행 차량의 안전 운행을 위협할 수 있으며, 특히 센서 융합 기반 판단 시스템에서도 위조된 위치 정보를 정탐지로 오인할 가능성이 존재한다.

3.2 HackRF one

HackRF One[3]은 범용 소프트웨어 정의 무선(SDR, Software Defined Radio) 장비로, 1MHz부터 6GHz 대역까지 송수신이 가능한 저비용 SDR 하드웨어이다. GPS 스푸핑 실험에서는 공격자가 사전 녹음 또는 시뮬레이션된 위성 신호를 생성한 후, 이를 HackRF One 장비를 통해 송신함으로써 스마트폰 등의 GPS 수신기가 위조된 GPS 신호를 받아들이도록 한다.

본 연구에서는 오픈소스 기반의 GPS 신호 생성 도구인 GPS-SDR-SIM과 NASA에서 제공하는 RINEX 천체력 파일을 활용하여 실제 GPS 신호 형식에 준하는 위조 데이터를 생성하였다. 이렇게 생성된 신호는 HackRF One을 통해 송신되며, 실험 환경에서 스마트폰 GPS 수신기의 위치 정보를 조작하는 데 활용되었다.

IV. 이상 탐지 방법

본 연구는 차량 내부에 설치된 스마트폰에서 실시간으로 수신하는 GPS 데이터를 활용하여, 실시간으로 이상 여부를 판단하는 구조를 제안한다. 이 시스템은 그림 1과 같이 순차적으로 입력되는 위도(Latitude), 경도(Longitude), 고도(Altitude), 속력(Speed), 시간(Timestamp)을 기반으로 학습된 모델이 다음 시점의 GPS 정보를 예측하고 실제 GPS 정보와 비교하여 오차를 기반으로 이상 여부를 판단한다. 판단은 과거 오차의 누적 패턴을 반영한 AS(Anomaly Score)를 정의하고 예상 이동 거리와 시간 간격을 고려한 TH(Dynamic Threshold)와의 비교를 통해 수행된다.

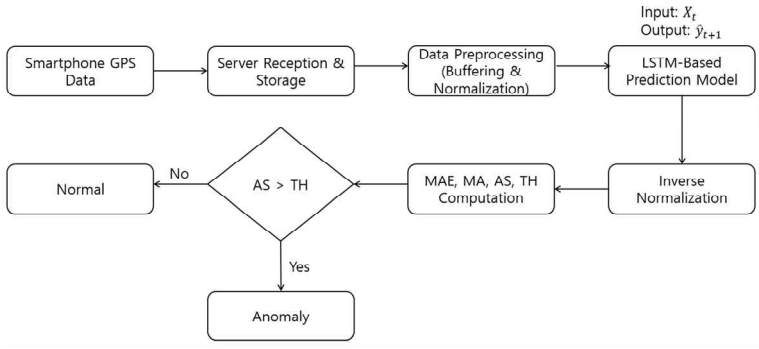

그림 1. 제안된 이상 탐지 방법
Fig. 1. Proposed approach

4.1 Data preprocessing

본 연구에서는 이상 탐지 모델의 학습을 위해 스마트폰의 GPS 수신기로부터 수집된 시계열 데이터를 기반으로 전처리 과정을 수행하였다. 원시 GPS 데이터는 위도(Latitude), 경도(Longitude), 고도(Altitude), 속력(Speed), 시간(Timestamp)을 포함한다. 이 중 모델 입력에 의미 있는 4개의 변수(Latitude, longitude, altitude, speed)를 특징(feature)으로 선택하였다.

이후 시계열 특성을 반영하기 위해 고정된 길이의 시퀀스를 생성하는 슬라이딩 윈도우 기법을 적용하였다. 구체적으로는 연속된 n개의 시점 데이터를 하나의 입력 시퀀스로 구성하고 해당 시퀀스 이후 시점의 데이터를 타겟 값으로 설정하여 입출력 쌍을 생성하였다. 이 과정을 통해 시계열 예측 학습에 적합한 형태의 훈련 데이터를 구성하였다.

또한, 입력 변수 간의 스케일 차이를 보정하고 학습 안정성을 향상시키기 위해 MinMaxScaler를 사용하여 각 변수의 값을 [0, 1] 범위로 정규화하였다. 이때 입력 시퀀스와 예측 대상 값 전체를 통합하여 Scaling 기준을 학습한 뒤, 같은 Scaler로 입력과 출력 데이터를 정규화하였다. 정규화된 데이터는 모델 학습 및 추론의 일관성을 유지하는 데 중요한 역할을 하며, 이는 후속 실험에서의 정밀한 이상 탐지를 가능하게 하였다.

이후 실시간 추론 및 이상 판단 과정에서는 모델이 예측한 결과와 실제 GPS 데이터를 비교하여 오차를 계산하고 이상 판단을 수행해야 하므로, 모델의 출력값에 대해서는 역정규화를 수행하여 원래의 GPS 단위로 복원한다. 이 과정을 통해 예측값과 실제값 간의 차이를 직관적인 수치로 비교할 수 있으며 이는 이후 이상 탐지 기준 계산의 기반이 된다.

4.2 Detection model

이상 탐지를 위한 예측 모델을 시계열 데이터의 시간 종속성을 효과적으로 모델링할 수 있는 LSTM(Long Short-Term Memory) 구조 [5] 를 기반으로 설계되었다. 입력은 과거 GPS 시계열 데이터의 연속된 시점을 사용하고 출력은 다음 시점의 GPS 값을 예측하는 방식이다. 입력 시퀀스는 위도(latitude), 경도(longitude), 고도(altitude), 속력(speed)의 4가지 요소로 구성되며, 총 5개의 시점의 연속된 데이터를 하나의 샘플로 구성하여 입력한다. 이를 수식으로 표현하면 다음과 같다. 식 (1)은 시점 t의 입력 시퀀스 S_t가 $t-4$부터 t까지 5개 시점의 연속된 GPS 벡터 X로 구성됨을 나타낸다. 여기서 시점 X_t는 시점 t의 GPS 벡터를 의미한다.

$$X_t = [x_{t-4}, x_{t-3}, x_{t-2}, x_{t-1}, x_t] \quad (1)$$

모델 출력, 즉 예측값은 식 (2)와 같다. 식 (2)는 학습된 LSTM 모델 f_θ가 입력 X_t를 받아, 다음 시점$(t+1)$의 위도, 경도, 고도, 속도인 $\hat{y}_{t+1}$를 예측하는 과정을 나타낸다.

$$\hat{y}_{t+1} = f_\theta(X_t) \quad (2)$$

첫 번째 입력 레이어는 (5, 4)의 시퀀스 형태의 데이터를 입력받으며, 여기서 5는 시퀀스의 길이, 4는 특징의 개수를 의미한다. 그 뒤를 이어 첫 번째 LSTM 레이어는 128개의 유닛을 가지며 해당 레이어에서는 시퀀스 전체를 출력으로 반환함으로써, 다음 레이어가 시계열 전체의 정보를 학습할 수 있도록 한다. 이어지는 Dropout 레이어에서 과적합을 방지하기 위해 일부 뉴런을 무작위로 제거한다.

다음으로 64개의 유닛을 가진 두 번째 LSTM 레이어는 마지막 시점의 은닉 상태만을 출력하며 이후에는 64차원의 Dense(Fully Connected) 레이어와 ReLU 활성화 함수를 적용하여 비선형성을 추가하고 복잡한 패턴을 학습할 수 있도록 설계하였다.

마지막 Dense(Fully Connected) 레이어는 4개의 출력 뉴런을 가지며 이는 다음 시점의 4가지 변수(latitude, longitude, altitude, speed)에 대한 예측값을 생성한다.

이후 상황별로 각 변수에 대해 차등 가중치를 적용한 평균제곱오차(Weighted MSE)를 계산하여 다양한 상황이나 환경별로 시스템 전반에 중요한 영향을 주는 변수에 가중치를 더욱 부여하여 모델이 해당 변수에 더욱 민감하게 반응함으로써 다양한 상황이나 환경별로 모델에 유동성을 부여할 수 있다. 학습은 Adam Optimizer와 함께 50 epoch 동안 수행되며, 손실 값이 개선되지 않을 경우 EarlyStopping callback을 적용하여 불필요한 과적합을 방지하였다.

4.3 Anomaly detection method

MAE(Mean Absolute Error)는 예측값 $\hat{y_i}$와 실제값 y_i사이의 절댓값 차이를 평균한 값으로, 특정 시점에서의 순간적인 예측 정확도를 측정하는 지표이다. 식 (3)은 시점 t에서의 MAE를 계산하는 과정을 나타낸다. n은 feature의 개수를, Y_i와 $\hat{Y_i}$은 각각 i번째 feature의 실제값과 예측값을 의미한다.

$$MAE = \frac{1}{n}\sum_{i=1}^{n}\left|\hat{Y_i} - Y_i\right| \tag{3}$$

본 연구에서는 시간(timestamp)를 제외한 위도(latitude), 경도(longitude), 고도(altitude), 속력(speed)의 GPS 데이터를 예측 대상으로 사용하며, 각각의 feature별 예측 오차를 모두 합산하여 평균을 구함으로써 한 시점의 전반적인 예측 성능을 수치화한다. MAE가 클수록 해당 시점의 예측이 실제 위치와 차이가 많이 난다는 뜻이며, 이는 스푸핑 공격 등 외부 요인에 의한 데이터 왜곡 가능성을 시사한다. 식 (4)는 최근 n개의 시점에서 측정된 MAE 값을 평균한 이동 평균값인 MA (Moving Average)를 나타낸다. 단일 시점이 아닌 일정 시간 구간 동안의 오차 흐름을 반영하여 이상 여부를 판단하는 데 사용된다. 수식에서 p_{t-i}는 시점 $t-i$에서 계산된 MAE 값이다. 이처럼 p는 시점별 예측 오차의 크기를 나타내며, MA는 이를 평균하여 오차의 시간적 추세를 반영한다.

$$MA_t = \frac{1}{n}\sum_{i=1}^{n}P_{t-i} \tag{4}$$

이 값은 노이즈나 일시적인 GPS 수신기의 오류에 의한 오탐지를 줄이기 위한 안정화 지표로 사용된다. MA가 클 경우, 일시적인 예외가 아니라 지속적인 예측 실패 또는 패턴 이탈이 발생하고 있음을 의미하며, 이는 시스템적으로 위험 징후가 누적되고 있다는 경고 신호로 간주될 수 있다. 식 (5)는 시점 t의 AS_t(이상 점수)가 해당 시점의 MAE_t와 MA_t의 산술 평균임을 나타낸다.

$$AS_t = \frac{MA_t + p_t}{2} \tag{5}$$

따라서, AS(Anomaly Score)는 MAE와 MA를 평균하여 계산한 지표로, 순간 예측 오차인 MAE와 과거 누적 오차 흐름인 MA를 동시에 반영한 이상도 지표이다. 단순한 오차 감지가 아닌, 시간적 연속성을 고려하여 보다 안정적이고 신뢰도 높은 이상 판단을 가능하게 한다. AS는 GPS 데이터가 급변하거나 패턴이 점진적으로 왜곡되는 상황에서 민감하게 반응할 수 있으면서도, 순간적인 이상치(노이즈, GPS 수신기의 오차 등)에만 휘둘리지 않도록 설계되어 있다. 식 (6)은 시점 t의 동적 임계값인 TH_t를 계산하

는 식을 나타내며, a는 오차 허용 기울기, b는 기본 허용 오차이다.

$$TH = a \times v \times \Delta t + b \quad (6)$$

AS는 단순히 고정된 임계값과 비교하는 것이 아닌 차량의 상태에 따라 실시간으로 계산되는 TH (Dynamic Threshold)와 비교되어 이상 판단을 수행한다. 임계값은 현재 차량 속력인 v와 GPS 수신 시점 간 시간 간격인 Δt를 기반으로 선형 함수 형태로 설정되며, a는 속력 및 시간에 따른 오차 허용 기울기로 속력이 클수록, 시간 간격이 넓을수록 GPS 오차는 자연스럽게 커지기 때문에 임계값을 선형적으로 확장해 주는 민감도를 조절하는 계수이다. b는 기본 허용 오차로 속력이 0이거나 시간 간격이 작을 때에도 기본적으로 허용해야 하는 오차 값을 보장한다. 이는 GPS 수신기 자체의 오차나 환경에 따른 편차 등을 고려한 최소 허용 범위이다. 본 연구에서 데이터 기반 보정 계수인 a와 b는 공개 데이터셋을 기반으로 그리드 서치(Grid search)로 결정하였으며, 검증 성능(F1 기준)에 따라 최종값을 a = 1.6, b = 4.7로 설정하였다. 식 (7)은 식 (5)에서 계산된 AS_t가 식 (6)에서 계산된 TH를 초과하는 경우에 해당 시점을 이상(Anomaly)으로 판단함을 의미한다.

$$AS_t > TH \quad (7)$$

V. 실 험

5.1 Normal data

GPS 스푸핑 공격의 방식은 매우 다양하고 임의적이며, 실제 차량 주행 중 대부분의 공격 방식에 대한 데이터를 충분히 확보하는 것이 현실적으로 어렵기 때문에 정상 데이터만 수집하고, 정상 데이터로만 학습하는 비지도 학습 기반의 이상 탐지 모델을 설계하였다.

정상 데이터는 실제 도로 주행 상황에서 차량 내부의 설치된 스마트폰의 GPS 수신기를 통해 수집되었다. GPS 데이터는 해당 스마트폰에서 일정 시간마다 수집되었으며, 수집되는 GPS 데이터는 위도(latitude), 경도(longitude), 고도(altitude), 속력(speed), 시간(timestamp) 의 정보를 포함하고 있다.

5.2 Attack scenario

Attack Scenario에서는 정상 GPS 데이터로 학습된 모델을 실제 스푸핑 공격 환경에 적용하여 실시간 이상 탐지 성능을 평가하는 실험을 수행하였다. 실시간 이상 탐지는 정상 데이터 수집 방식과 동일하게 주행 중인 차량 내부에 설치된 스마트폰으로부터 수신되는 GPS 데이터를 실시간으로 수집하고 처리한다.

Attack Scenario는 실제 스푸핑 환경을 모사하기 위해, 차량 내부에 설치된 HackRF One 장비를 사용하여 조작된 GPS 신호를 스마트폰에 송출하는 방식으로 진행되었다. GPS 스푸핑 공격 시나리오 생성을 위해 오픈소스로 제공되는 GPS 신호 시뮬레이터인 GPS-SDR-SIM 도구를 사용하였으며[10], 해당 도구는 실제 위성의 궤도 정보에 기반한 GPS 신호 생성을 위해 NASA의 CDDIS(Crustal Dynamics Data Information System)에서 제공하는 GNSS Daily RINEX 파일을 참조하여 GPS 스푸핑 신호를 구성하였다[11].

HackRF One을 이용한 GPS 스푸핑 공격은 실제 경로와 비슷하지만 점진적으로 편향된 경로를 따라가도록 하는 공격 방식과 실제 경로와 멀리 떨어진 경로를 따라가도록 하는 공격 방식으로 설계되었으며, 공격 시 스마트폰의 GPS 수신기는 정상 신호와 유사하면서도 상대적으로 세기가 강한 위조된 GPS 신호를 신뢰하고 수신함으로써 위조된 위치를 실제 위치로 인식하게 된다.

이러한 실험은 기존의 정적 로그 기반 평가 방식과 달리 차량 주행 중 실시간으로 변화하는 위치 정보에 따라 모델이 어떻게 반응하고 이상 판단을 수행하는지를 현실적인 조건 하에서 동적으로 검증할 수 있다는 점에서 중요한 의의를 가진다. 실험 과정 전반에서 이상 탐지 판단은 데이터를 받아오는 즉시 수행되며, 각 시점에 대한 결과는 로그 파일로 저장되어 사후 분석 등에 활용되었다.

5.3 실험 결과

본 연구의 실험은 i7-14700HX, RTX 4060 GPU, 32GB RAM, Windows11을 탑재한 노트북과 삼성 Galaxy Ace, Galaxy J5, Galaxy M12 스마트폰을 활용하였다. 실시간 GPS 수신 및 서버 전송은 Flask 기반 서버 애플리케이션을 통해 구성되었고, GPS 스푸핑 공격은 HackRF One 장비와 Kali Linux 환경에서 GPS-SDR-SIM 도구를 사용하여 생성하였다. 실험은 GPS 신호 간섭을 최소화하기 위해 제한된 공간과 통제 가능한 공간에서 수행되었으며, 다양한 센서 융합 요소가 제외된 단일 GPS 기반 판단 환경에서 진행되었다.

본 연구에서는 제안된 모델의 GPS 이상 탐지 효과를 평가하기 위해 두 단계의 성능 검증을 수행하였다. 1차 평가는 수집된 정상 데이터에 임의의 공격 데이터를 삽입한 정적 로그 데이터를 기반으로 모델의 탐지 성능을 정량적으로 검증하였고, 2차 평가에서는 차량 주행 중 실시간으로 수집된 GPS 데이터를 이용하여 모델의 실시간 이상 탐지 성능을 검증하였다.

성능 검증을 위해 사용된 평가 지표로는 TP(True Positive), FN(False Negative), FP(False Positive), TN(True Negative)이 있으며, 이를 바탕으로 Accuracy, Precision, Recall, F1-score, FPR(False Positive Rate)을 계산하여 성능을 평가하였다.

Accuracy는 전체 데이터 중에서 모델이 올바르게 분류한 데이터의 비율을 나타내며, 모델의 전반적인 분류 성능을 평가하는 지표이다. Precision은 모델이 비정상으로 판단한 데이터 중에서 실제로 비정상인 데이터의 비율을 의미하며, 탐지된 이상 데이터의 신뢰도를 나타낸다. Recall은 전체 실제 비정상 데이터 중에서 모델이 올바르게 탐지한 비정상 데이터의 비율로, 이상을 얼마나 놓치지 않고 탐지하는지를 보여주는 지표이다. F1-score는 Precision과 Recall의 조화 평균으로, 두 지표 간 균형을 고려하여 모델의 이상 탐지 성능을 종합적으로 평가하는 데 사용된다. 마지막으로 FPR은 실제 정상 데이터 중에서 모델이 비정상으로 잘못 판단한 비율을 의미하며, 오탐지의 가능성을 나타내는 지표이다.

표 1과 그림 2는 정상 데이터와 GPS 스푸핑 공격 데이터가 포함된 정적 로그 데이터를 기반으로 수행된 1차 평가의 결과이며, 해당 실험에서는 공개 데이터셋을 활용하였다. 해당 실험에서는 AV-GPS-Dataset [12], 경기도 자율주행센터의 GPS 데이터셋[13], 한국전자통신연구원(ETRI)에서 제공되는 GPS 데이터셋[14]을 사용하였다. 각 데이터셋은 위도, 경도, 고도, 속도 등 핵심 위치, 운동 정보와 타임스탬프를 포함하며, 도심, 간선도로, 고속도로 등 다양한 주행 환경을 포괄한다.

이 평가는 학습된 모델이 정적 로그 데이터셋 상에서 이상 탐지 성능을 얼마나 잘 수행하는지를 확인하기 위한 실험으로 GPS 시계열 데이터의 전반적인 경향성과 공격 패턴에 대한 탐지 정확도를 수치적으로 분석하였다. 평가 결과, Accuracy 98.52%, Precision 95.42%, Recall 98.97%, F1-score 97.16%, 그리고 FPR 1.63%를 기록하였으며, 이는 높은 정밀도와 재현율을 동시에 확보함으로써 오탐과 미탐을 모두 효과적으로 억제하는 성능을 실험적으로 입증하였다.

표 1. 정적 로그 데이터 기반 모델 성능 평가 결과
Table 1. Performance evaluation results based on static log data

TP	15,593	Accuracy	0.9852
FN	162	Precision	0.9542
FP	749	Recall	0.9897
TN	45,227	F1-score	0.9716
		FPR	0.0163

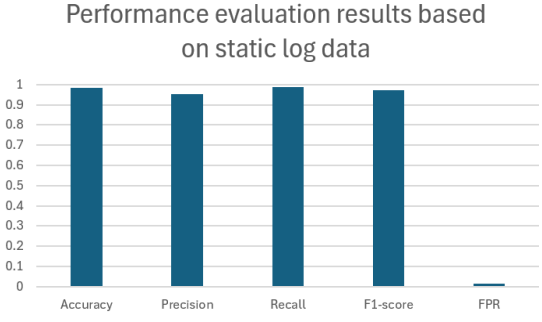

그림 2. 정적 로그 데이터 기반 모델 성능 평가 결과
Fig. 2. Performance evaluation results based on static log data

표 2와 그림 3은 실시간 이상 탐지 성능을 평가하기 위해 차량 내부에 설치된 스마트폰에서 실시간으로 수신되는 GPS 데이터를 기반으로 수행된 2차 평가의 결과를 나타낸다. 이 평가는 실제 차량 주행 환경에서 서버로 전송되는 실시간 데이터를 바탕으로 이상 탐지가 수행되는 과정을 그대로 반영하고 있으며, 모델의 실시간 응답성과 환경 변화에 대한 적응성을 중점적으로 검증하였다.

표 2. 실시간 GPS 데이터 기반 모델 성능 평가 결과
Table 2. Performance evaluation results based on real-time GPS data

TP	9,896	Accuracy	0.9896
FN	104	Precision	0.9765
FP	238	Recall	0.9896
TN	16,024	F1-score	0.9827
		FPR	0.0146

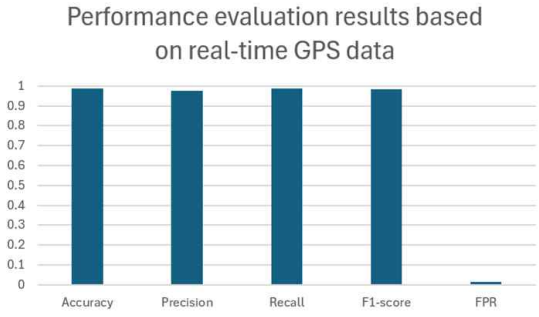

그림 3. 실시간 GPS 데이터 기반 모델 성능 평가 결과
Fig. 3. Performance evaluation results based on real-time GPS data

실험 결과, Accuracy 98.96%, Precision 97.65%, Recall 98.96%, F1-score 98.27%, 그리고 FPR 1.46%를 기록하였으며, 이는 정적 로그 데이터 기반 평가와 유사한 수준의 우수한 성능을 유지함과 동시에 실시간 처리 환경에서도 안정적으로 GPS 스푸핑을 탐지할 수 있음을 보여준다.

이러한 결과는 제안한 모델이 실시간 환경에서의 이상 탐지에 적합하며, 자율주행 차량 등 높은 신뢰성과 즉각적인 대응이 요구되는 시스템에 적용 가능함을 실험적으로 입증한 것이다. 다만, 실제 환경에서는 GPS 신호나 GPS 수신기의 일시적 불안정이나 자연적 변동성으로 인해 일부 오탐(False positive)과 미탐(False negative)이 발생할 가능성도 존재한다. 예를 들어, 고층 건물 밀집 지역, 터널 내부, 또는 급격한 환경 변화 구간에서는 신호 왜곡이 자연스럽게 발생할 수 있으며, 이는 정상 주행 중임에도 이상으로 오인되는 사례로 이어질 수 있다. 이러한 점은 GPS 기반 단일 센서 구조의 한계에서 기인한 것으로, 향후에는 추가적인 센서 융합이나 맥락 정보 반영 등을 통해 보완될 필요가 있다.

본 연구는 일반 스마트폰의 GPS 수신기를 활용하여 데이터를 수집하였기 때문에 정밀 RTK 수준의 고정밀 측위는 불가능하며, 일부 데이터는 수신 환경에 따라 노이즈가 포함될 수 있다. 또한, HackRF One을 활용한 스푸핑 공격은 공공장소에서의 사용 제한으로 인해 차폐된 공간 또는 외부 간섭이 적은 환경에서만 수행되었으며, 실제 자율주행 차량의 센서 융합 기반 판단 환경을 완전히 재현하지는 못하였다. 더불어, 본 연구는 데이터 부족의 이유로 비지도 학습 기반으로 정상 데이터만을 학습에 활용하였기 때문에, 탐지하지 못하는 GPS 스푸핑 공격이 존재할 수 있다. 이러한 제한점을 보완하기 위해서는 향후 연구에서 센서 융합 기반의 데이터 통합, 다양한 이상 유형을 포괄하는 지도 학습 기반 구조, 그리고 복잡한 실세계 환경에 대한 시뮬레이션 확대가 필요할 것으로 판단된다.

VI. 결론 및 향후 과제

본 연구에서는 자율주행 차량 환경에서 발생할 수 있는 GPS 스푸핑 공격에 대응하기 위한 실시간 이상 탐지 시스템을 제안하고 구현하였다. 기존 GPS 스푸핑 탐지 연구들이 정적 로그 데이터 기반 분석이나 센서 융합 등 하드웨어 의존적인 방식에 집중되어있는 반면 본 연구는 스마트폰의 GPS 수신 데이터를 활용한 순수 소프트웨어 기반 접근으로, 실제 차량 주행 환경에서 실시간 탐지 성능을 실험적으로 입증하였다는 점에서 차별성을 가지며, 실제 자율주행 차량 시스템에 적용 가능성을 보였다.

제안된 시스템은 LSTM 기반 시계열 예측 모델을 통해 정상적인 GPS 데이터 흐름을 학습하고, 실시간으로 수신된 GPS 데이터와의 차이를 바탕으로

이상 여부를 판단한다. 이 과정에서 MAE, MA, AS를 기반으로 한 복합적인 탐지 기준과 동적 임계값 적용을 통해 일시적인 오차나 환경 변화로 인한 오탐지를 최소화하고 지속적인 패턴 이탈이나 공격에 대한 민감한 반응을 가능하게 하였다. 또한 HackRF One을 활용해 실제 GPS 스푸핑 공격을 구성하고, 주행 중인 차량 내부에 설치된 스마트폰에서 실시간 GPS 데이터를 수신하여 이상 탐지 실험을 진행함으로써 현실적인 공격 시나리오를 구성하여 탐지 정확도와 실시간 응답성을 검증하였다.

모델의 성능 평가는 정적 로그 데이터를 기반으로 한 1차 평가와 차량 주행 중 실시간 데이터를 활용한 2차 평가로 나누어 진행하였다. 평가 결과 높은 성능과 낮은 FPR을 기록함으로써, 실시간 환경에서도 신뢰성 있는 이상 탐지가 가능함을 입증하였다.

향후 연구에서는 본 연구에서 제안한 이상 탐지 시스템을 보다 확실하게 자율주행 시스템에 적용하기 위해 다양한 현실적 조건과 공격 방식을 반영하여 실험을 확장하여 수행할 계획이다. 다양한 경로 편향 방식, 속도 및 고도 기반 교란, 다중 위성 신호 간섭 등 보다 정교하고 비정형적인 스푸핑 공격 기법을 반영하여 보다 다양한 공격 기법에 대응할 수 있도록 하며, 도심, 지하, 터널, 개활지 등 GPS 수신 환경이 상이한 주행 조건에서의 탐지 성능을 분석하고 향상시켜 모델의 환경 적응성과 범용성을 강화할 계획이다.

References

[1] S. Dasgupta, A. Ahmed, M. Rahman, and T. Bandi, "Unveiling the stealthy threat: Analyzing slow drift GPS spoofing attacks for autonomous vehicles in urban environments and enabling the resilience", arXiv preprint, arXiv:2401.01394, Jan. 2024. https://doi.org/10.48550/arXiv.2401.01394.

[2] GPS World – Two years since the Tesla GPS hack, https://www.gpsworld.com/two-years-since-the-tesla-gps-hack. [accessed: Jul. 03, 2025]

[3] Great Scott Gadgets – HackRF One, https://greatscottgadgets.com/hackrf/one. [accessed: Jul. 03, 2025]

[4] D. Kiruthikaa and G. Ananthi, "AHLSTM: Attention-Enabled Hierarchical LSTM Autoencoder Framework for detecting GPS Spoofing Attacks in Autonomous Vehicles", SSRN preprint, Sep. 2024.

[5] B. Wang, W. Li, and Z. H. Khattak, "Anomaly detection in connected and autonomous vehicle trajectories using LSTM autoencoder and Gaussian mixture model", Electronics, Vol. 13, No. 7, pp. 1251, Apr. 2024. https://doi.org/10.3390/electronics13071251.

[6] M. M. Abrar, M. Rahman, and M. Chowdhury, "GPS-IDS: Anomaly-based GPS spoofing attack detection framework for autonomous vehicles", Electronics, Vol. 13, No. 6, pp. 1013, Mar. 2024. https://doi.org/10.3390/electronics13061013.

[7] K. Lee, H. Jung, and S. Lee, "Anomaly Detection Method of User Trajectories based on Deep Learning Technologies", Journal of Korea Institute of Information Technology, Vol. 20, No. 11, pp. 101-116, Nov. 2022. http://doi.org/10.14801/jkiit.2022.20.11.101.

[8] P. Stojković and P. Tadić, "Object Location Prediction in Real-time using LSTM Neural Network and Polynomial Regression", arXiv preprint, arXiv:2311.13950, Nov. 2023. https://doi.org/10.48550/arXiv.2311.13950.

[9] S. Dasgupta, M. Rahman, M. Islam, and M. Chowdhury, "Prediction-based GNSS spoofing attack detection for autonomous vehicles", Proc. IEEE Int. Conf. on Intelligent Transportation Systems (ITSC), Rhodes, Greece, pp. 1-7, Sep. 2020. https://doi.org/10.1109/ITSC45102.2020.9294582.

[10] osqzss, "gps-sdr-sim", GitHub repository, https://github.com/osqzss/gps-sdr-sim. [accessed: Jun. 17, 2025].

[11] NASA CDDIS GNSS Daily RINEX Files, https://cddis.nasa.gov/archive/gnss/data/daily/. [accessed: Jun. 17, 2025]

[12] Mehrab Abrar, "AV-GPS-Dataset: Autonomous Vehicle GPS spoofing dataset", GitHub repository, https://github.com/mehrab-abrar/AV-GPS-Dataset. [accessed: Jun. 11, 2025]

[13] Gyeonggi Autonomous Driving Center, "Pangyo Zero City Real-World Autonomous Driving GPS Trajectory Dataset", GeoMarket, https://geomarket.kr/user/dataset/view.do?data_sn=18. [accessed: Jun. 11, 2025]

[14] Electronics and Telecommunications Research Institute (ETRI), "Vehicle Trajectory Dataset for Autonomous Driving Technology Development (Genesis G80-based GPS/IMU + Mobileye Sensor)", Korea Public Data Portal, https://www.data.go.kr/data/15041797/fileData.do. [accessed: Jun. 11, 2025]

저자소개

강 태 훈 (Taehun Kang)

2021년 3월 ~ 현재 : 전북대학교 소프트웨어공학과 학사과정

2025년 1월 ~ 현재 : 전북대학교 지능형보안연구실 연구원

관심분야 : 지능형보안, 인공지능, LLM, 이상 탐지

최 선 오 (Sunoh Choi)

2005년 2월 : 고려대학교 컴퓨터학과(이학사)

2014년 5월 : Purdue Univ. 컴퓨터공학부(공학박사)

2014년 8월 ~ 2019년 2월 : ETRI 정보보호본부 선임연구원

2021년 3월 ~ 현재 : 전북대학교 소프트웨어공학과 부교수

관심분야 : 지능형 보안, 데이터보안, 네트워크보안