Journal of KIIT. Vol. 22, No. 12, pp. 257-265, Dec. 31, 2024. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2024.22.12.257

CAN 데이터 기반 예측 모델을 활용한 차량 이상 탐지

이용준*[1], 김성광*[2], 최선오**

Anomaly Detection in Vehicles using Predictive Models based on CAN Data

Yongjoon Lee*[1], Seongkwang Kim*[2], and Sunoh Choi**

이 논문은 2024년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된
지자체-대학 협력기반 지역혁신 사업의 결과입니다(2023RIS-008)

요 약

CAN 통신은 보안 메커니즘이 없어 데이터 위조, 변조와 같은 사이버 공격에 취약하다. 특히 최근 테슬라 모델X의 블루투스 해킹 사례처럼, 보안이 미흡한 경우 해킹을 통해 차량을 조작하거나 훔치는 일이 발생할 수 있다. 이러한 공격으로부터 시스템을 보호하고 데이터 무결성을 보장하기 위해 CAN 통신에서 이상 행위를 실시간으로 탐지할 수 있는 예측 기반 모델이 필요하다. 본 연구에서는 현대자동차의 파비스에서 직접 CAN 데이터를 추출하고 추출된 데이터를 활용하여 예측기반 이상 탐지 모델을 학습하고 주행 데이터의 실제 값과 예측 값을 비교하여 성능평가를 진행한다. 단변량 예측 모델과 다변량 예측 모델의 성능 비교 분석하여 각 예측 모델의 정확도를 제시한다.

Abstract

The CAN communication protocol lacks built-in security mechanisms, making it vulnerable to cyber-attacks such as data falsification and modification. In particular, as illustrated by the recent Bluetooth hacking incident with the Tesla Model X, inadquate security can allow malicious actors to manipulate or steal vehicles. To safeguard systems from such attacks and ensure data integrity, a predictive model capable for real-time anomaly detection within CAN communication is essential. This study utilizes CAN data extracted directly from Hyundai's Pavis model to train a prediction-based anomaly detection model. Performance evaluation is conducted by comparing the actual driving data with the predicted values. Also the performance of univariate and multivariate predictive models is compared and analyzed to present the accuracy of each predictive model.

Keywords
CAN communication, anomaly detection, vehicle security, predictive model, deep learning

* 전북대학교 소프트웨어공학과 학사과정
- ORCID[1]: https://orcid.org/0009-0005-2841-8008
- ORCID[2]: https://orcid.org/0009-0001-2643-6019
** 전북대학교 소프트웨어공학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-0654-7109

· Received: Nov. 12, 2024, Revised: Dec. 03, 2024, Accepted: Dec. 06, 2024
· 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

현재 자동차는 수십 개의 전자제어장치(ECU, Electronic Control Unit)들로 구성되어 각 제어기들은 각기 다른 기능을 담당하며 자동차의 핵심 시스템을 제어한다[1]. 대표적으로 엔진을 제어하는 엔진을 제어하는 엔진 제어 장치(ECU, Engine Contorl Unit), 변속기를 제어하는 변속기 제어 장치(TCU, Transmission Control Unit), 운전 보조 시스템(ADAS, Advanced Driver Assistance System) 등이 있다. 각 제어기들은 빠르고 정확하게 데이터를 주고받아 차량 내 다양한 장치들의 작동을 돕는다.

자동차 내에서 주로 사용되는 통신 프로토콜에는 CAN(Controller Area Network), LIN(Local Interconnect Network), MOST(Multimedia Oriented System Transport) 등이 있다[2]. 특히 CAN 통신은 가장 널리 사용되는 프로토콜로서 차량 내에서 중앙 컴퓨터 없이 개별 마이크로컨트롤러와 장치들이 직접 통신하기 위해 설계된 표준 통신 규격이다[3].

CAN 버스는 실시간 제어 능력을 갖춘 통신 기술로, 자동차의 엔진, 브레이크, 안전 장치, 멀티미디어 기기 등 다양한 부품의 통합 운영에 핵심적인 역할을 한다. ISO 11898 표준을 준수하며, 고속 CAN(High-Speed CAN)과 저속 CAN(low-Speed CAN)으로 나뉜다[4].

이러한 CAN 버스는 설계 당시 보안보다는 효율성과 단순성에 중심을 두었기 때문에, 오늘날 다양한 사이버 공격에 취약한 구조를 가지고 있다[5].

자동차 해킹을 통해 공격자는 차량의 네트워크에 접근하여 임의의 데이터를 삽입하거나 기존 데이터를 조작하여 차량의 정상적인 동작을 방해하는 메시지 위조, 서비스 거부 공격 등을 수행할 수 있다. 대표적인 예로 차량 운행 중 RPM을 조작하여 차량의 속도를 올리거나 차량의 문을 열어 탈취하는 공격을 할 수 있다. 특히 차량의 중요 제어 기능에 영향을 미치는 ECU들을 탈취할 경우 탑승자의 안전에 심각한 위험을 가할 수 있다[6].

CAN 통신의 보안 측면의 취약점은 차량 내 핵심 시스템을 보호하는 보안 시스템의 필요성을 부각한다. CAN 통신을 악용한 공격이 발생할 경우 차량 및 탑승자의 안전이 크게 위협받을 수 있기 때문에 CAN 통신에 특화된 보안 시스템을 통해 비정상적인 행동 및 보안 위협을 탐지하고 차단하는 것이 필수적이다[7].

이상탐지는 정상적인 데이터 패턴에서 벗어나는 비정상적인 행동이나 이벤트를 식별할 수 있다. 차량 내 CAN 통신에서는 다양한 ECU들이 주고받는 데이터를 이상탐지를 통해 패턴에서 벗어나는 데이터를 감지하여 보안 위협을 발견할 수 있다. 이를 통해 차량의 정상적인 동작을 방해하는 공격을 탐지하고 신속하게 대응할 수 있다[8].

딥러닝 기반 이상탐지 모델은 CAN 통신의 복잡한 패턴을 학습하고 비정상적인 행동을 정교하게 탐지할 수 있는 방법 중 하나이다. 특히 LSTM은 시계열 데이터의 연속적인 흐름을 학습하여 과거 정보를 바탕으로 현재와 미래의 상태를 예측하는 데 뛰어난 성능을 발휘한다. 이를 통해 차량의 통신 패턴에서 미세한 변화를 감지하여 다양한 보안 위협에 대한 탐지 정확도를 높일 수 있다[9].

본 논문에서는 차량의 CAN 데이터를 활용하여 딥러닝 기반 이상탐지 모델을 소개하고자 한다. 제안하는 모델은 LSTM을 활용하여 차량 내 비정상적인 데이터를 탐지하고 이를 통해 CAN 통신에서 발생할 수 있는 보안 위협에 대해 신속하고 효과적으로 대응할 수 있는 시스템을 구현하는 것을 목표로 한다.

Ⅱ. 관련 연구

2.1 원격 프레임을 이용한 차량 내 네트워크 침입 탐지 기법

H. Lee et al.[10]은 차량 내 CAN 네트워크에 대한 침입 탐지 시스템으로 OTIDS(On-board Time Interval-based Detection System)를 제안하였다. OTIDS는 차량 내 통신에서 발생하는 원격 프레임의 오프셋 비율과 요청-응답 메시지 사이의 시간 간격을 분석하여 보안 위협을 탐지한다. 정상 상태에서는 각 노드가 일정한 응답 오프셋 비율과 시간 간격을 유지한다는 점을 활용한다.

실제 기아 Soul 차량의 OBD-Ⅱ 포트에서 수집한 CAN 트래픽 데이터셋을 사용하여 OTIDS의 유효성을 검증했으며 데이터셋에는 정상 상태와 함께 DoS 공격, 퍼지 공격, 가장 공격 등의 시나리오가 포함되어 있다. 이 데이터셋을 기반으로 제안한 방법의 유효성을 검증하였으며 높은 정확도로 빠른 침입 탐지가 가능함을 보였다.

2.2 CNN을 사용한 이상탐지 기법

Y. Li et al.[11]은 차량 네트워크의 사이버 공격 취약성을 해결하기 위해 CNN 기반 침입 탐지 시스템(IDS)를 제안하였다. VGG16, VGG19, Inception 등 최신 CNN 모델을 사용하고 PSO(Particle Swarm Optimization) 기법을 적용하여 성능을 최적화한 결과, Car-Hacking 및 CICIDS2017 데이터셋에서 99.25% 이상의 탐지율과 F1-score를 기록하였다. 이는 CNN의 공간적 패턴 학습 능력을 활용한 결과이다.

반면, 본 연구에서는 CAN 데이터의 시간적 연속성을 유지하며 이상 패턴을 탐지하기 위해 LSTM(Long Short-Term Memory)을 사용한다. CNN이 데이터의 공간적 패턴 학습에 적합한 반면, LSTM은 시계열 데이터를 직접 처리하여 시간적 상관관계를 활용할 수 있다는 장점이 있다. 본 연구는 이러한 특성을 기반으로 LSTM이 CAN 데이터에서 정밀한 이상 탐지를 가능하게 함을 입증하고자 한다.

2.3 CAN 버스 공격 방지를 위한 메시지 인증 및 키 분배 메커니즘

A.-R. Cho et al.[5]은 CAN 통신의 보안 취약점을 해결하기 위한 보안 프레임워크를 제안하였다. 인증서 관리, 키 분배 및 업데이트, CAN 메시지 인증 프로토콜로 구성된다. 각 ECU는 인증서를 통해 비밀값을 안전하게 수신하여 세션키와 인증키를 생성하고 카운터를 통해 재전송 공격을 방지한다.

또한 사용되지 않는 CAN Data 필드 일부를 활용해 59 비트의 메시지 인증 코드를 포함하며 AES-CTR로 5바이트의 데이터를 암호화하여 스니핑 공격을 방지한다. 이 메커니즘은 실시간성과 보안성을 동시에 제공하고 있다.

Ⅲ. 자동차 이상탐지 방법

3.1 데이터 수집

본 연구에서는 CAN 통신에서 발생하는 정상 및 비정상 데이터를 학습하기 위해 현대 파비스(Hyundai Pavis) 차량을 대상으로 데이터를 수집하였다[12].

데이터를 수집하기 위해 CAN 네트워크 분석 도구인 CANoe를 사용하였다[13]. CANoe는 Vector사에서 개발한 통합 개발 및 시뮬레이션 도구로 차량 내 네트워크 시스템의 개발, 테스트, 분석 및 시뮬레이션에 활용된다. 이 도구를 통해 CAN 버스 상의 메시지를 모니터링하고 기록하여 네트워크의 동작을 분석할 수 있다. CANoe에서 수집한 필드는 AccelPedalPos1, EngSpeed, WheelBasedVehicleSpeed 세 가지다. 각 데이터의 의미는 다음과 같다.

3.1.1 AccelPedalPos1

가속 페달 위치를 나타내는 값이다. 운전자가 가속 페달을 얼마나 밟고 있는지 나타낸다. 해당 값이 높을수록 가속 페달이 더 많이 밟힌 것을 의미한다[14].

3.1.2 EngSpeed

엔진 속도를 나타내며 일반적으로 분당 회전수(RPM)로 측정된다. 이 값은 엔진이 얼마나 빠르게 회전하는지를 보여준다[14].

3.1.3 WheelBasedVehicleSpeed

바퀴 기반 차량 속도를 나타내는 값으로 차량의 계기판에 나오는 실제 속도를 의미한다. 이 값은 차량의 바퀴 회전을 기반으로 측정되며 주행 중 차량의 이동 속도를 파악하는 역할을 한다[15].

실험은 두 가지 주행 조건에서 수행되었다. 정상 주행 조건에서는 그림 1과 같이 차량을 정지 상태(0km/h)에서 출발하여 시속 60km/h까지 가속하였다. 시속 60km/h에 도달한 후 3분간 등속 주행을 유지한다.

주행 후에는 차량을 감속하여 정지한다. 이때 수집된 데이터는 차량의 안정적인 주행 패턴을 반영하는 정상 데이터로 정의한다.

우리는 이상탐지문제를 좀더 간단하게 만들기 위하여 차량을 가속하거나 감속하는데 소요되는 시간을 제외하였다.

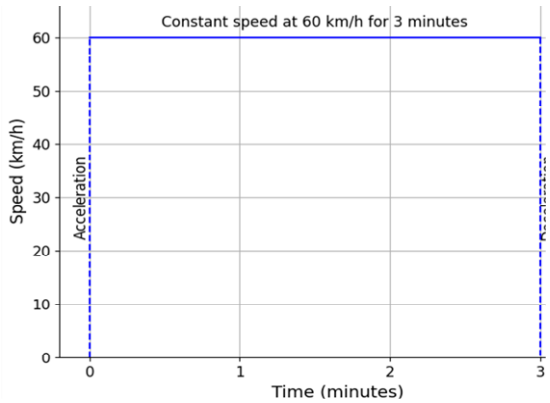

그림 1. 정상주행
Fig. 1. Normal driving

비정상 주행 조건은 그림 2와 같이 차량을 정지 상태(0km/h)에서 출발하여 시속 60km/h까지 가속한다. 시속 60km/h에 도달한 후 1분간 등속 주행을 유지한다. 그 다음, 차량의 속도를 시속 90km/h까지 다시 가속한다. 시속 90km/h에 도달한 후 1분간 등속 주행을 유지한다. 주행 후에는 차량을 감속하여 정지한다. 이때 수집된 데이터는 급격한 속도 변화와 비정상적인 주행 패턴을 반영하는 이상 데이터로 정의한다.

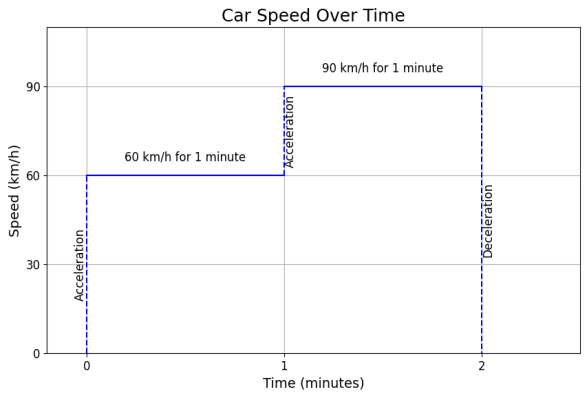

그림 2. 비정상주행
Fig. 2. Abnormal driving

이와 같은 설정을 통해 CAN 통신에서 정상과 비정상 패턴을 구분할 수 있는 데이터를 확보하고 이를 기반으로 비정상 주행을 실시간으로 탐지할 수 있는 딥러닝 기반 이상 탐지 모델을 구축하고자 한다.

3.2 데이터 기본 분석

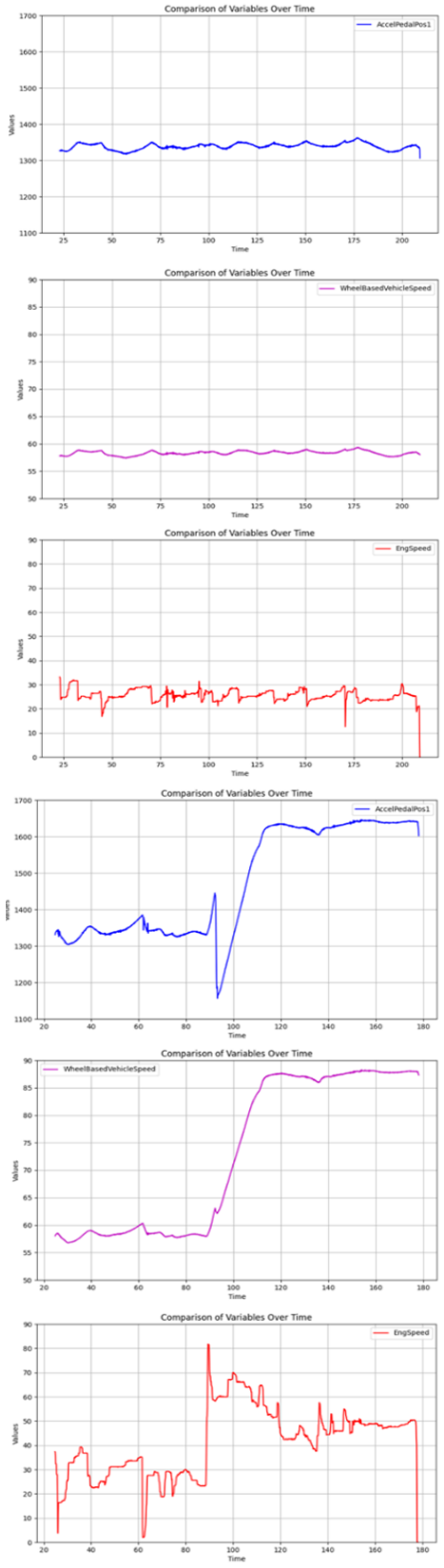

그림 3. 3개 필드의 정상데이터 및 이상데이터
Fig. 3. Normal data and abnormal data in three fields

그림 3은 정상 주행(왼쪽)과 이상 주행(오른쪽) 시 각 변수 AccelPedalPos1, EngSpeed, WheelBasedVehicleSpeed 의 시간 변화에 따른 변화를 비교한 그래프이다.

첫 번째 행의 그래프는 AccelPedalPos1의 변화를 보여준다. 정상 주행에서는 AccelPedalPos1 값이 일정하게 유지되고 큰 변동이 없는 패턴을 보인다. 반면 이상 주행 시에는 주행 도중 값이 급격히 상승하는 패턴이 나타난다. 급격히 상승하는 패턴 이전에 하강하는 부분은 차량의 기어 변속으로 인해 일어난 것으로 예상된다.

두 번째 행의 그래프는 WheelBasedVehicleSpeed의 변화를 보여준다. 정상 주행에서는 속도가 안정적으로 유지되지만, 이상 주행 시에는 특정 시점에서 급격한 상승이 발생하고 이후에도 높은 값으로 유지된다. 이는 차량 속도가 비정상적으로 증가하는 상황을 반영하여 이상 주행 상태의 특성을 나타낸다.

세 번째 행의 그래프는 EngSpeed의 변화를 보여준다. 정상 주행에서는 EngSpeed가 일정 범위 내에서 유지되며 비교적 안정적인 패턴을 보인다. 반면 이상 주행에서는 EngSpeed가 급격히 상승했다가 변동을 반복하는 불안정한 패턴을 보인다. 이상 주행 시 급가속으로 인하여 기어가 바뀌어 엔진회전수가 변한 것으로 추측된다.

이 그래프들을 통해 정상 주행과 이상 주행 간에 변수들의 뚜렷한 차이가 나타남을 확인할 수 있으며 각 변수의 급격한 변화가 이상 주행을 탐지하는 데 중요한 지표로 활용될 수 있음을 알 수 있다.

그림 4와 5는 각각 정상 주행과 이상 주행 시의 각 필드 별 상관계수를 나타낸 것이다. 정상 주행 시 AccelPedalPos1과 WheelBasedVehicleSpeed는 0.99의 높은 상관계수를 보여 두 변수 간의 강한 상관관계를 보여준다. 반면 EngSpeed는 AccelPedalPos1과 WheelBasedVehicleSpped와의 상관계수가 각각 -0.023, -0.056으로 낮아 정상 주행 상태에서 독립적인 특성을 나타낸다.

이상 주행 시에는 AccelPedalPos1 과 WheelBasedVehicleSpeed 간의 상관계수는 0.96으로 여전히 높은 수준을 유지하고 있다. EngSpeed와 다른 변수들 간의 상관계수는 각각 0.43, 0.6로 증가하였다. 이는 차량이 저속 주행 후 고속 주행으로 가속하는 시점으로 인해 다른 변수들과의 상관성이 높아졌음을 의미한다.

	AccelPedalPos1	EngSpeed	WheelBasedVehicleSpeed
AccelPedalPos1	1	-0.023	0.99
EngSpeed	-0.023	1	-0.056
WheelBasedVehicleSpeed	0.99	-0.056	1

그림 4. 정상데이터에서의 필드간 상관관계
Fig. 4. Correlation between fields in normal data

	AccelPedalPos1	EngSpeed	WheelBasedVehicleSpeed
AccelPedalPos1	1	0.43	0.96
EngSpeed	0.43	1	0.6
WheelBasedVehicleSpeed	0.96	0.6	1

그림 5. 이상데이터에서의 필드간 상관관계
Fig. 5. Correlation between fields in abnormal data

3.3 모델 학습

본 연구에서는 차량 운행 데이터를 활용하여 LSTM 모델을 기반으로 한 예측 모델을 학습하였다.

해당 모델은 장기 및 단기 패턴을 효과적으로 학습할 수 있다. LSTM의 핵심 구조는 게이트 메커니즘으로, 과거 시점의 중요한 정보를 유지하면서 불필요한 정보를 망각하게 한다[16].

이러한 특성은 차량 운행 데이터와 같이 시간적 연속성이 중요한 데이터에서 이상 행동을 탐지하는 데 적합하다.

LSTM을 사용하는 이상 탐지 방법은 정상적인 시계열 패턴을 학습한 모델이 새로운 입력 데이터의 예상값을 예측하고, 이를 실제 관측값과 비교하여 이상치를 탐지하는 방식으로 작동한다. 모델 학습 과정은 단변량 예측 모델과 다변량 예측 모델로 나누어 진행하였다.

이상탐지 모델에서는 정상데이터를 이용하여 모델을 학습한다. 따라서, 정상데이터와 유사한 데이터가 입력될 경우 모델의 예측값은 실제값과 유사하여 예측값과 실제값의 오차가 작다. 그러나, 정상데이터와 다른 이상현상이 발생할 경우 정상데이터로 학습한 모델의 예측값은 이상현상의 실제값과 오차가 크게 된다. 따라서, 우리는 모델의 예측값과 실제값의 차이가 임계치보다 클 경우 이상현상이 발생한 것으로 판단할 수 있다.

단변량 예측 모델은 차량의 속도를 의미하는 WheelBasedVehicleSpeed 변수를 입력 데이터로 사용하여, 다음 시점에서의 속도를 예측하는 LSTM 모델이다. 이 모델은 속도 변화에 대한 시계열 패턴을 학습하여 속도의 급격한 변화나 이상치를 탐지하는 데 활용된다.

다변량 예측 모델은 AccelPedalPos1, WheelBasedVehicleSpeed, EngSpeed 총 3개의 변수를 입력으로 사용하여각 변수의 다음 시점 값을 예측하는 LSTM 모델이다. 이 모델은 다변량 시계열 데이터를 통해 변수 간 상관관계를 학습해 여러 변수의 변화를 반영하여 예측을 수행하도록 한다.

학습에 사용된 시계열 데이터는 슬라이딩 윈도우 방식을 사용하여, 이전 시점의 데이터를 기반으로 다음 시점 값을 예측하도록 모델을 학습하였다 [17]. 이 방식은 입력 데이터에서 일정한 크기의 윈도우를 순차적으로 이동시키면서 학습 데이터와 예측 목표 값을 구성하는 방법으로, 시계열 데이터의 순차적 특성을 유지하면서 효과적으로 패턴을 학습할 수 있다.

슬라이딩 윈도우 방식에서 윈도우 크기는 10으로 설정하였다. 한 번에 10개의 연속된 시계열 데이터를 하나의 입력 시퀀스로 사용하며, 시점 t-9 부터 시점 t 까지의 데이터를 입력으로 사용하고, 이 입력에 이어지는 시점 t+1 의 값을 예측 목표 값으로 설정한다. 이러한 방식을 활용해 단변량 및 다변량 LSTM 모델을 학습시켰으며, 이를 통해 비정상적 패턴을 탐지하고자 한다.

성능평가를 위해 공격을 가정한 데이터에 60km/h와 90km/h의 중간 값인 75km/h이상을 악성으로 판단하고 라벨링을 하였다.

3.4 학습 결과

단변량 예측 모델의 경우, anomaly score는 모델이 예측한 속도와 실제 속도 간의 차이를 기반으로 계산된다. 그림 6에서와 같이 혼동 행렬을 구하기 위한 threshold는 F1 score가 가장 높은 지점으로 설정하였으며, 그 결과 F1 score: 1.0, precision: 1.0, recall: 1.0으로 모든 정상 및 이상 데이터를 정확히 구별할 수 있었다. Threshold는 0.252 으로 설정되었다.

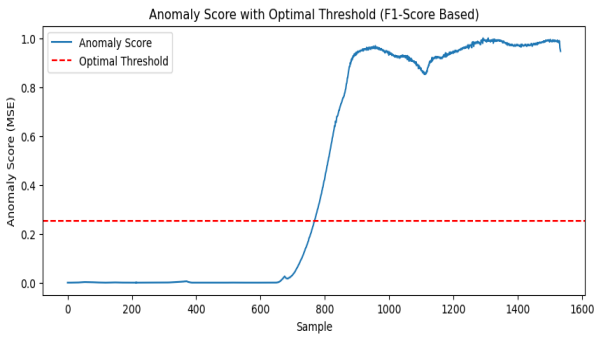

그림 6. 단변량 예측 모델 결과
Fig. 6. Univariate prediction model results

반면, 다변량 예측 모델에서는 AccelPedalPos1, WheelBasedVehicleSpeed, EngSpeed 세 가지 변수의 예측값과 실제값 간의 차이 합을 anomaly score로 설정하였다. 혼동 행렬을 구하기 위한 threshold는 동일하게 F1 score가 가장 큰 지점으로 설정하였으며, 그 결과 F1 score: 0.936, precision: 0.882, recall: 0.997의 성능을 나타냈다. Threshold는 0.221으로 설정되었다.

단변량 예측 모델과 다변량 예측 모델을 비교한 결과, 다변량 예측 모델보다 단변량 예측 모델이 더

높은 성능을 보였으며 단변량 모델은 F1 score, precision, recall 모두 1.0을 기록하였다.

이는 다변량 예측 모델의 경우 엔진 RPM 값이 학습에 사용되는데, 속도가 증가할 때 기어 변속에 의해 RPM 값이 오히려 감소하는 구간이 발생하기 때문이다. 모델은 기어 변속을 고려하지 못하여 예측값과 실제값 간에 큰 오차가 발생하게 되었고, 이로 인해 다변량 예측 모델의 성능이 상대적으로 떨어진 것으로 분석된다.

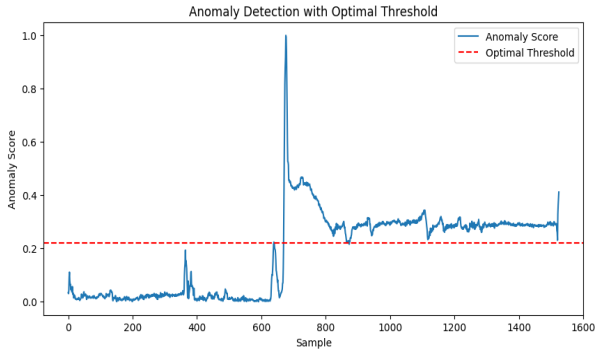

그림 7. 다변량 예측 모델 결과
Fig. 7. Multivariate prediction model results

3.5 향후 과제

다변량 예측 모델의 성능을 개선하기 위해 주행 시 발생하는 기어 변속과 같은 복잡한 주행 패턴을 반영하는 방안을 연구할 필요가 있다. 이는 기어 변속 시점과 RPM 변화 간의 관계를 모델이 학습할 수 있는 추가적 레이어나 주행 조건 변수를 모델에 포함하여 학습의 정확도를 높일 계획이다.

본 연구에서는 일부 변수만을 사용하여 모델을 학습하였으나, 차량의 주행 환경과 같은 외부 요인을 반영하는 다변량 모델을 구축함으로써 예측 성능과 이상 탐지 정확도를 향상시킬 계획이다. 다양한 주행 조건에서 성능을 유지할 수 있는 모델을 개발함으로써, 차량의 안전성을 강화하고 실시간 주행 상황에서도 이상을 탐지할 수 있는 성능을 높이고자 한다.

Ⅳ. 결 론

본 연구에서는 CAN 통신 데이터를 활용하여 차량의 정상 및 비정상 주행 패턴을 구분하고 이상 탐지를 수행할 수 있는 LSTM 기반 예측 모델을 제안하였다. 실험에서는 단변량 예측 모델과 다변량 예측 모델을 각각 설계하여 성능을 비교하였으며, F1 score 기반의 threshold를 설정하여 두 모델의 이상 탐지 성능을 평가하였다.

실험 결과, 단변량 예측 모델은 모든 정상 및 이상 데이터를 구분하였고, 다변량 예측 모델과 비교했을 때 더욱 우수한 성능을 나타냈다. 다변량 예측 모델은 변수간 상호작용을 반영할 수 있는 장점이 있지만, 기어 변속과 같은 특정 주행 상황에서 발생하는 비선형적 변화를 정확하게 예측하지 못하여 성능이 다소 낮아졌다.

References

[1] V. Siddhartha V, S. Yaji, and N. Kalappa, "Comparison of CAN, LIN, FLEX RAY and MOST in-vehicle bus protocols", Journal of Emerging Technologies and Innovative Research (JETIR), Vol. 6, No. 4, pp. 160-165, Apr. 2019.

[2] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes", 2008 IEEE 68th Vehicular Technology Conference, Calgary, AB, Canada, pp. 1-5, Sep. 2008. https://doi.org/10.1109/VETECF.2008.259.

[3] Y.-K. Kim, K.-R. Ryu, and C.-W. Hur, "A Study on Transmission Protocol for Controller Area Network", Proc. of the Korean Institute of Information and Commucation Sciences Conference, pp. 836-838, May 2010.

[4] D. Y. Choi, Y. H. Yoon, J. H. Oh, and S. E. Lee, "High-Speed CAN-FD Controller for In-Vehicle Network", Journal of the Institute of Electronics and Information Engineers, Vol. 56, No. 12, pp. 109-116, Dec. 2019. https://doi.org/10.5573/ieie.2019.56.12.109.

[5] A.-R. Cho, H.-J. Jo, S. Woo, Y.-D. Son, and D.-H. Lee, "A Message Authentication and Key

Distribution Mechanism Secure Against CAN Bus Attack", Journal of the Korea Institute of Information Security & Cryptology, Vol. 22, No. 5, pp. 1057-1068, Oct. 2012. https://doi.org/10.13089/JKIISC.2012.22.5.1057.

[6] OCSLab, "CAN intrusion dataset", Hacking & Countermeasure Research Lab, https://ocslab.hksecurity.net/Dataset/CAN-intrusion-dataset [accessed: Nov. 30, 2024]

[7] S. Hong, "Research on Countermeasures of Controller Area Network Vulnerability", Journal of Convergence for Information Technology, Vol. 8, No. 5, pp. 115-120, Oct. 2018. https://doi.org/10.22156/CS4SMB.2018.8.5.115.

[8] S. Lee and W. Choi, "Periodic-and-on-Event Message-Aware Automotive Intrusion Detection System", Journal of the Korea Institute of Information Security & Cryptology, Vol. 31, No. 3, pp. 373-385, Jun. 2021. https://doi.org/10.13089/JKIISC.2021.31.3.373.

[9] I. Sucholutsky, A. Narayan, M. Schonlau, and S. Fischmeister, "Deep Learning for System Trace Restoration", 2019 International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, Jul. 2019. https://doi.org/10.1109/IJCNN.2019.8852116.

[10] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A Novel Intrusion Detection System for in-vehicle Network by using Remote Frame", 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, Canada, Aug. 2017. https://doi.org/10.1109/PST.2017.00017.

[11] Li Yang, Abdallah Shami , "A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles", IEEE International Conference on Communications (ICC), 2022. 10.1109/ICC45855.2022.9838780

[12] Hyundai Motor Company, "Pavise - Exterior Gallery", Hyundai Motor Company, https://www.hyundai.com/kr/ko/c/products/truck/pavise/gallery-detail/exterior [accessed: Nov. 11, 2024]

[13] Vector Informatik GmbH, "CANoe Product Information", https://www.vector.com/kr/ko/products/products-a-z/software/canoe/ [accessed: Nov. 11, 2024]

[14] B. Park, B. Joo, K. Jung, and J. Park, "A Case Study on the Application of SEooC to Evaluate Hardware Element for the Accel Pedal Sensor", Vol. 29, No. 7, pp. 609-620, Mar. 2020. http://dx.doi.org/10.7467/KSAE.2021.29.7.609.

[15] C. K. Song, M. Uchanski and J. K. Hedrick., "Vehicle Speed Estimation Using Accelerometer and Wheel Speed Measurements", SAE Technical Paper, pp. 1-10, Jul. 2002. https://doi.org/10.4271/2002-01-2229.

[16] Jeong, J. (2021). A study on occupancy detection method using indoor temperature, relative humidity, CO_2 , and illuminance values. Journal of the Korean Institute of Information Technology (JKIIT), 19(6), 81-88. 10.14801/jkiit.2021.19.6.81

[17] C. Zhao, H. Dang, Y. Wang, J. Wei, and K. Honda., "Individual Variation of Morphological and Acoustic Effects of the Nasal Tract", 2013 IEEE China Summit and International Conference on Signal and Information Processing, Beijing, China, Jul. 2013. https://doi.org/10.1109/ChinaSIP.2013.6625356.

저자소개

이 용 준 (Yongjoon Lee)

2019년 3월 ~ 현재 : 전북대학교 소프트웨어공학과 학사과정

2023년 7월 ~ 현재 : 전북대학교 지능형보안연구실 연구원

관심분야 : 지능형보안, 자동차 보안, 데이터분석, 인공지능

김 성 광 (Seongkwang Kim)

2020년 3월 ~ 현재 : 전북대학교 소프트웨어공학과 학사과정
2024년 1월 ~ 현재 : 전북대학교 지능형보안연구실 연구원
관심분야 : 지능형보안, 자동차 보안, 리버스 엔지니어링

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 : 자동차보안, 원자력보안, 지능형보안