ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 24-01-02
6

j.inst.Korean.electr.electron.eng.Vol.28,No.1,6~13,March 2024
https://doi.org/10.7471/ikeee.2024.28.1.6

가우시안 커널 밀도 추정 함수를 이용한 오토인코더 기반 차량용 침입 탐지 시스템

Autoencoder-Based Automotive Intrusion Detection System Using Gaussian Kernel Density Estimation Function

김 동 현*, 임 형 철*, 이 성 수*★

Donghyeon Kim*, Hyungchul Im*, and Seongsoo Lee*★

Abstract

This paper proposes an approach to detect abnormal data in automotive controller area network (CAN) using an unsupervised learning model, i.e. autoencoder and Gaussian kernel density estimation function. The proposed autoencoder model is trained with only message ID of CAN data frames. Afterwards, by employing the Gaussian kernel density estimation function, it effectively detects abnormal data based on the trained model characterized by the optimally determined number of frames and a loss threshold. It was verified and evaluated using four types of attack data, i.e. DoS attacks, gear spoofing attacks, RPM spoofing attacks, and fuzzy attacks. Compared with conventional unsupervised learning-based models, it has achieved over 99% detection performance across all evaluation metrics.

요 약

본 논문에서는 비지도학습 모델인 오토인코더와 가우시안 커널 밀도 추정 함수를 이용하여 차량용 CAN 네트워크에서 비정상적인 데이터를 탐지하는 방안을 제안한다. 제안하는 오토인코더 모델은 정상 데이터에서 CAN 프레임의 ID만으로 학습시킨다. 이후 가우시안 커널 밀도 추정 함수를 이용하여 구한 최적의 프레임 개수와 손실 임계값을 가지는 모델을 사용하여 비정상 데이터를 효과적으로 탐지한다. DoS 공격, Gear 스푸핑 공격, RPM 스푸핑 공격, Fuzzy 공격 등 4가지 공격 데이터로 오토인코더 기반 IDS를 검증하였으며 성능을 평가하였다. 기존 비지도학습 기반 모델들과 비교했을 때 우수한 성능을 나타냈으며 모든 평가 지표에서 99% 이상의 성능을 나타냈다.

Key words : Automotive, Autoencoder, Controller Area Network, Deep Learning, Intrusion Detection System, Unsupervised Learning, Gaussian Kernel Density Estimation

---

* School of Electronic Engineering and Department of Intelligent Semiconductor, Soongsil University (Student, Student, Professor)
★ Corresponding author
E-mail : sslee@ssu.ac.kr, Tel : +82-2-820-0692
※ Acknowledgment
This work was supported by the R&D Program of the Ministry of Trade, Industry, and Energy (MOTIE) and Korea Evaluation Institute of Industrial Technology (KEIT) (RS-2022-00155731, RS-2023-00232192). It was also supported by MOTIE and Korea Institute for Advancement of Technology (KIAT) (P0012451). The authors wish to thank Em. Prof. Boo-Gyoun Kim for his comments and discussions and IC Design Education Center (IDEC) for CAD support. Manuscript received Mar. 18, 2024; revised Mar. 22, 2024; accepted Mar. 25, 2024.

Ⅰ. 서론

최근 자동차 산업에서 전자 제어 장치(ECU: Electronic Control Unit)의 사용이 증가하면서, 차량 네트워크 보안이 매우 중요한 이슈로 부상하고 있다[1]. 차량 네트워크의 핵심은 ECU 간의 데이터 송수신을 관리하는 CAN (Controller Area Network) 통신 시스템에 있다. CAN 통신은 차량 내 다양한 전자 시스템 사이의 효율적인 통신을 가능하게 하고, 멀티 마스터 구조를 통해 모든 노드가 데이터 전송을 시작할 수 있는 유연성을 제공한다. 하지만 CAN 통신은 송수신하는 노드의 주소가 정해져 있지 않으며, 암호화 같은 보안 기능이 없어 공격에 취약한 구조이다. 이러한 CAN 통신의 취약성을 악용하여 차량의 오작동을 유발하는 공격이 보고되었다[2].

CAN 통신의 취약성을 보완하기 위해 다양한 침입 탐지 시스템(IDS: Intrusion Detection System)이 제안되고 있다. 먼저, 머신러닝 기반으로 서포트 벡터 머신(Support Vector Machine)을 사용하여 정상 및 공격 프레임을 탐지하는 방법[3], 최근접 이웃 알고리즘(Nearest Neighbour Algorithm)을 이용하는 방법[4], 랜덤 포레스트(Random Forest)를 이용하는 방법[5] 등이 제안되었다. 또한 딥러닝 방식을 적용하여 CAN 공격을 탐지하는 방안이 제안되었다[6][7]. 하지만 이와 같은 지도학습 기반 IDS는 학습되어 있는 공격 탐지에만 유효하며, 새로운 유형의 공격이 발생할 경우 탐지가 불가능하다는 단점이 존재한다. 따라서 이를 해결하기 위해 GAN (Generative Adversarial Networks)을 이용하는 비지도학습 기반 IDS가 제안되었다[8]. 또한 iForest(Isolation Forest)를 이용하여 학습되지 않은 공격을 탐지하는 방안이 제안되었다[9]. 하지만 이와 같은 비지도학습 기반 IDS는 지도학습 기반 IDS와 비교했을 때, 성능이 낮다는 단점이 존재한다. 또한 NovelADS를 이용한 비지도학습 기반 IDS가 제안되었다[10]. 이는 성능은 우수하지만 각각의 공격 유형에 대하여 서로 다른 임계값을 정해야 한다는 단점이 존재한다.

또한 오토인코더 모델을 기반으로 한 다양한 IDS가 제안되었다[11]. [12]는 CNN(Convolutional Neural Network)과 LSTM(Long Shot-Term Memory)을 결합하여 오토인코더의 인코더 및 디코더 계층으로 사용한 IDS를 제안하였으며 [13], [14]는 LSTM을 이용한 오토인코더 기반의 IDS를 제안하였다. [15]는 SRCAE(Sparse Regularization Convolutional Autoencoder)와 스트림 클러스터링 모델을 결합한 IDS를 제안하였으며 [16]은 Attention Mechanism과 오토인코더를 이용한 IDS를 제안하였다. [17]에서는 DCAEs(Deep Contractive Autoencoders)기반의 IDS를 제안하였고 [18]에서는 GRU (Gated Recurrent Unit) 기반의 오토인코더를 적용한 IDS를 제안하였으며 [19]에서는 GAN과 합성곱 오토인코더(Convolutional Autoencoder)를 결합한 CAAE (Convolutional Adversarial Autoencoder)기반 IDS를 제안하였다.

본 논문에서는 가우시안 커널 밀도 추정 함수를 사용하여 최적의 프레임 개수와 임계값을 구하고 이를 사용한 오토인코더 기반 IDS를 제안한다. 제안하는 모델은 비지도학습 기반으로 먼저 정상적인 CAN 트래픽만을 이용하여 학습시킨다. 다음으로 공격이 포함된 CAN 트래픽을 이용하여 공격을 효과적으로 탐지할 수 있음을 확인하였다. 또한 기존에 제안되어 있는 비지도학습 모델들보다 성능이 우수함을 시뮬레이션으로 검증하였다.

Ⅱ. 오토인코더 기반 침입 탐지 시스템

1. 데이터 세트 및 데이터 전처리

본 논문에서는 Hacking and Countermeasure Research Lab에서 제공하는 차량 해킹 데이터 세트[20]을 사용하였다. 이 데이터 세트는 정상 CAN 프레임만이 포함된 정상 데이터 세트, DoS(Denial of Service) 공격 데이터 세트, Gear 스푸핑(Spoofing) 공격 데이터 세트, RPM 스푸핑 공격 데이터 세트, 퍼지(Fuzzy) 공격 데이터 세트의 다섯 가지로 구성되어 있다. [20]에서 4가지의 공격 데이터 세트에는 표 1과 같이 공격 프레임과 정상 프레임이 함께 존재하며 이를 사용하여 학습을 진행하였다.

먼저 DoS 공격은 의도적으로 높은 우선순위의 ID를 가진 CAN 프레임을 주입시켜 지속적으로 CAN 버스를 점유하고, 정상 노드들의 데이터 송수신을 방해한다. 스푸핑 공격은 CAN 트래픽을 분석 및 리버싱(reversing)

Table 1. Overview of the car hacking dataset [20].
표 1. 차량 해킹 데이터 세트[20]의 구성 정보

Attack Type	# of Total Frame	# of Normal Frame	# of Attack Frame
DoS attack	3,665,771	3,078,250	587,521
Fuzzy attack	3,838,860	3,347,013	491,847
Gear attack	4,443,142	3,845,890	597,252
RPM attack	4,621,702	3,966,805	654,897

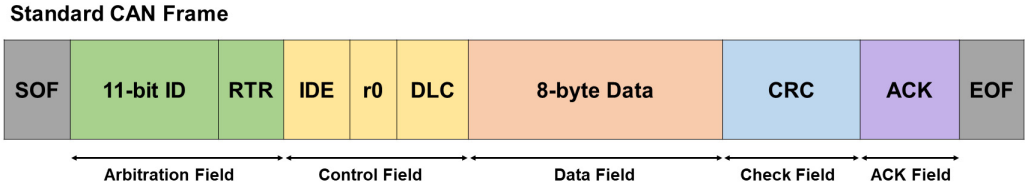

Fig. 1. Structure of CAN data frame.
그림 1. CAN 데이터 프레임 구조

하여 RPM 및 Gear와 같이 특정 장치와 관련된 ID를 주입함으로써 차량을 의도적으로 조작하는 공격이다. 마지막으로 퍼지 공격은 랜덤하게 ID와 데이터를 생성하여 주입시키는 공격이다. 이 과정에서 실제로 차량에서 사용되는 ID가 주입되면 차량의 장치가 오작동하게 된다. 또한 무작위로 CAN 버스를 점유하게 되어 노드간의 정상적인 데이터 송수신을 방해하게 된다.

본 논문에서는 공격이 포함되어 있지 않은 정상 데이터에서 CAN ID만을 추출하여 학습에 사용하였다. CAN 데이터 프레임의 ID는 그림 1과 같이 11비트로 구성되어 있으며, 정상 데이터에 포함된 총 988,872프레임의 CAN ID를 추출한 뒤 N개의 프레임씩 그룹화하여 (N, 11) 크기의 2차원 데이터를 학습에 사용하였다. 이때 N의 값은 11부터 64까지 변화시키며 총 54가지의 방법으로 학습을 진행하였다. Train 데이터와 Validation 데이터로는 N개의 프레임씩 그룹화한 정상 데이터를 2:1의 비율로 나누어 사용하였다. 테스트 데이터로는 DoS 공격 데이터, Gear 스푸핑 공격 데이터, RPM 스푸핑 공격 데이터, 퍼지 공격 데이터 등 총 4가지의 공격 유형을 각각 N×11 크기로 전처리하여 사용하였다.

2. 제안하는 오토인코더 모델

본 논문은 공격 데이터를 학습하지 않고 정상 데이터만을 학습하여 공격을 효과적으로 탐지하는 모델을 제안한다. 따라서 전통적인 지도학습(Supervised Learning) 방법이 아닌 비지도학습(Unsupervised Learning) 방법을 사용한다.

가. 오토인코더(Autoencoder)

오토인코더는 인코더와 디코더 두 부분으로 구성된 비지도학습 모델이다. 이 모델은 데이터의 잠재적 특성을 학습하는데 효과적이며, 이를 통해 정상적인 데이터 패턴과 이상 패턴을 구별하는 데 사용된다. 먼저, 인코더는 입력 데이터를 받아 완전 연결층(Fully-Connected Layer)을 통해 이를 저차원의 잠재 공간으로 압축한다. 반대로 디코더는 이 저차원 잠재 공간에서 데이터를 다시 완전 연결층을 통해 원래의 형태로 복원하는 작업을 수행한다.

본 논문에서 제안하는 오토인코더의 구조를 그림 2에 나타내었다. 인코더는 단일 Flatten Layer와 Dense Layer로 구성된다. Flatten Layer에서는 (N, 11) 크기의 2차원 데이터를 입력받아 N×11개의 유닛으로 출력한다. 인코더의 Dense Layer에서는 N×11개의 유닛을 입력받아 64개의 유닛으로 압축시킨다. 이때, 활성화 함수로 ReLU를 사용하여 비선형 변환을 수행한다. 디코더는 Dense Layer와 Reshape Layer로 구성된다. 디코더의 Dense Layer에서는 64개의 유닛으로 압축된 데이터를 입력받아 N×11개의 유닛으로 출력한다. 여기서 Dense Layer는 활성화 함수로 Sigmoid를 적용하여 데이터의 복원을 진행한다. 최종적으로 Reshape Layer가 Nx11개의 유닛을 입력받아 (N, 11) 크기의 2차원 데이터를 출력하게 된다.

나. 하이퍼파라미터 설정

본 논문에서는 오토인코더의 손실 함수로 평균 제곱오차(Mean Squared Error, MSE)를 선택하였고 이를 식 (1)에 나타내었다. MSE는 입력 데이터와 재구성된 데

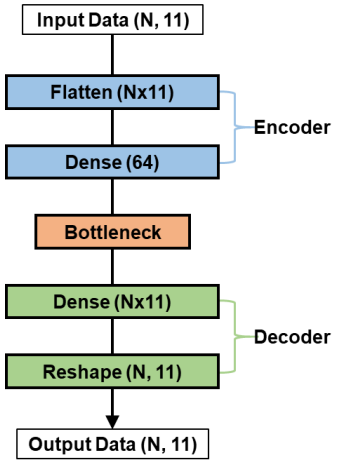

Fig. 2. Structure of the proposed autoencoder.
그림 2. 제안하는 오토인코더의 구조

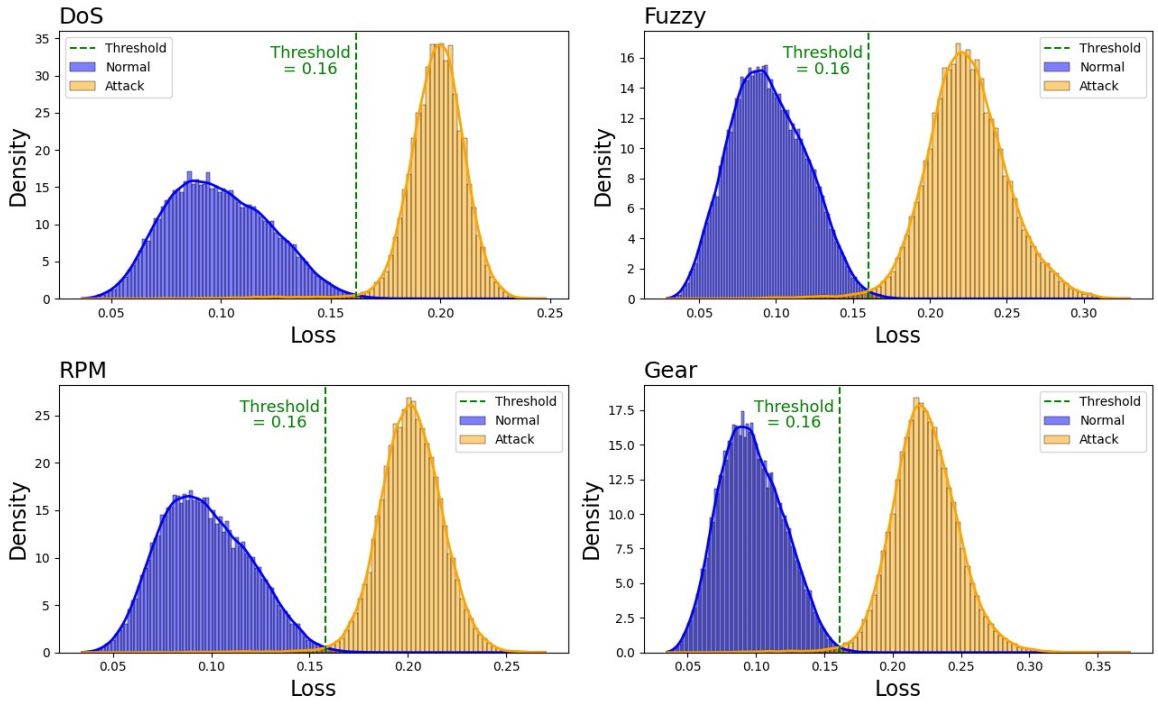

Fig. 3. Distribution of autoencoder loss by attack type using Gaussian KDE function with N value of 49.
그림 3. N값이 49일 경우의 가우시안 커널 밀도 추정 함수를 이용한 오토인코더의 공격 유형별 손실값 분포

이터 간의 차이를 정량화하는 데에 효과적이다. 특히 오토인코더의 경우, 데이터 재구성의 정확성이 중요하므로 MSE는 이를 측정하는 데 적합한 손실함수이다.

$$MSE = \frac{1}{n_m}\sum_{i=1}^{n_m}(y_i - \hat{y_i})^2 \quad (1)$$

여기에서 y_i는 실제 값, $\hat{y_i}$는 예측된 값, n_m은 샘플의 총 개수를 의미한다. 따라서 식 (1)을 통해 모델의 성능을 정확하게 평가하고, 오토인코더의 인코딩 및 디코딩 과정을 최적화할 수 있다.

또한 제안하는 오토인코더 모델을 최적화하기 위해 학습률(Learning Rate)을 0.001로 설정하고 옵티마이저를 Adam으로 설정하였다. Adam 옵티마이저는 효율적인 계산과 뛰어난 수렴 속도 덕분에 널리 사용된다. 이러한 설정은 모델의 학습 과정을 최적화하고 효과적인 성능 향상을 위해 중요한 역할을 한다.

Ⅲ. 실험 결과

1. 임계값 설정 및 최적의 프레임 개수 결정

본 논문에서는 오토인코더를 통해 얻은 손실값을 기반으로 임계값을 설정하였다. 이는 데이터 전처리 과정에서 사용된 CAN 프레임 개수(N)와 밀접한 관련이 있다. 먼저, 학습된 오토인코더 모델에 공격 데이터를 입력하였을 때 출력되는 손실값의 분포를 나타내기 위해 가우시안 커널 밀도 추정(Gaussian KDE: Gaussian Kernel Density Estimation)함수를 사용하였고, 본 논문에서는 이를 식 (2)와 같이 KDE로 표현한다.

$$KDE(x) = \frac{1}{n_k h}\sum_{i=1}^{n_k} K_g\left(\frac{x - x_i}{h}\right) \quad (2)$$

여기에서 K_g는 가우시안 커널 함수, n_k는 정상 혹은 공격 데이터에 해당하는 손실값들의 개수, h는 밴드폭, x_i는 손실값을 나타낸다.

N값이 49일 때 식 (2)를 이용하여 4가지의 공격 데이터 세트에 대해 구한 손실값 분포를 그림 3에 나타내었다. 여기에서의 정상(Normal)은 N개의 CAN 프레임 중에 공격 프레임이 단 하나도 포함되지 않았을 때를 나타낸다. 또한 공격(Attack)은 N개의 CAN 프레임 중 한 개 이상의 공격 프레임이 포함되어 있을 때를 나타낸다.

본 논문에서 공격과 정상을 나누는 임계값은 정상의 손실값 분포 그래프와 공격의 손실값 분포 그래프의 교점으로 결정하였다. 즉 임계값을 두 KDE 함수가 교차하는 지점의 손실값으로 정의한다. 이를 식 (3)에 나타내었다.

$$Threshold = \arg\min_{x} |KDE_0(x) - KDE_1(x)| \quad (3)$$

여기서 $KDE_0(x)$와 $KDE_1(x)$은 각각 정상과 공격에 대한 가우시안 커널 밀도 추정 함수를 나타낸다. 따라서 $\arg\min_{x} |KDE_0(x) - KDE_1(x)|$는 $KDE_0(x)$와 $KDE_1(x)$가 같아지는 x를 나타낸다. 4가지 공격 유형에 대하여 같은 임계값을 가지는 프레임 수 N이 존재하면 그러한 N을 가지는 모델은 4가지 공격 유형이 존재하는 환경에서 모든 공격 유형에 대하여 우수한 성능을 가진다. 따라서 N 값을 11부터 64까지 변화시켜가며 4가지 공격 유형에 대한 임계값을 구하였고 그 결과를 그림 4에 나타내었다. N이 커질수록 임계값이 커짐을 볼 수 있으며 총 8개의 N값에서 4가지 공격 유형의 임계값이 같음을 볼 수 있었다. 8개의 N값은 표 2에 나타내었다.

표 2의 N값 중 최적의 프레임 개수를 찾기 위해 본 논문에서는 정상을 공격으로 판단하는 확률과 공격을 정상으로 판단하는 확률의 합을 오류율 추정값으로 선택하였다. 오류율 추정값이 최소화되는 N을 가지는 모델이 프레임을 잘못 판단할 확률이 작아지기 때문에 우수한 성능을 보이리라고 판단하였다. 오류율 추정값을 구하기 위하여 사용한 식은 식(4)와 같다.

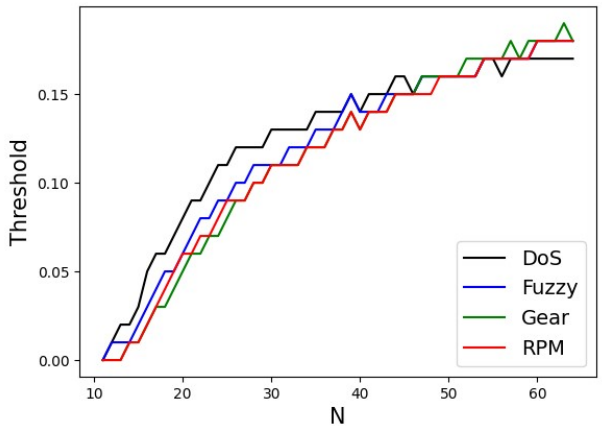

Fig. 4. Threshold by attack type according to N.
그림 4. N에 따른 공격 유형별 임계값

$$Error\ Rate\ Estimation = \frac{\int_{-\infty}^{L_{Th}} KDE_1(x)dx}{\int_{-\infty}^{\infty} KDE_1(x)dx} + \frac{\int_{L_{Th}}^{\infty} KDE_0(x)dx}{\int_{-\infty}^{\infty} KDE_0(x)dx} \quad (4)$$

여기서 L_{Th}는 식(3)에서 구한 임계값이다. $\int_{-\infty}^{L_{Th}} KDE_1(x)dx$를 $\int_{-\infty}^{\infty} KDE_1(x)dx$로 나눈 식은 공격을 정상으로 판단한 확률을 의미한다. 또한 $\int_{L_{Th}}^{\infty} KDE_0(x)dx$를 $\int_{-\infty}^{\infty} KDE_0(x)dx$로 나눈 식은 정상을 공격으로 판단한 확률을 의미한다. 따라서 이 두 확률의 합은 정상과 공격 데이터가 얼마나 구분이 잘 되는지에 대한 척도가 되며 이를 통해 잘못 탐지할 비율이 얼마나 낮은지 알 수 있다.

Table 2. N values yielding uniform thresholds for 4 types of attacks
표 2. 4가지 공격 유형에 대하여 임계값이 동일하게 나오는 N값

Values of N yielding uniform thresholds							
11	46	49	50	51	54	55	58

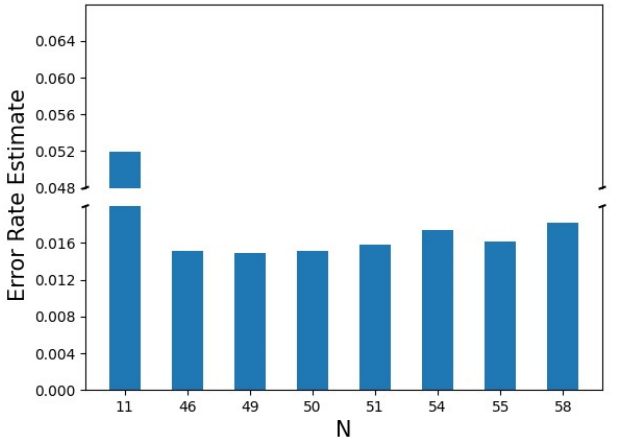

Fig. 5. Comparison of error rate estimate according to N.
그림 5. N에 따른 오류율 추정값 비교

표 2의 N값들에 대하여 식 (4)를 이용하여 4가지 공격 유형에 대하여 잘못 판단할 확률을 구한 뒤, 평균을 낸 값을 구하였고 그 결과를 그림 5에 나타내었다. 이를 통해 N이 49일 때 가장 작은 값을 가짐을 볼 수 있다. 따라서 N이 49일 때 4가지 공격 유형에 대하여 동일한 임계값을 가지며 또한 모델이 공격을 정상으로, 정상을 공격으로 잘못 판단할 확률을 최소로 가지게 되어 우수한 성능을 가진다고 판단된다.

2. 성능 평가

본 논문에서 제안하는 모델의 성능 평가를 표 3에 나타내었다. 표 3을 통해 기존에 제안되어 있는 지도학습 기반 IDS[7][19] 및 비지도학습 기반 IDS[8][9][10]과 성능을 비교하였다. 먼저 DCNN(Deep Convolutional Neural Network) 모델[7]은 지도학습 기반으로 공격

Table 3. Comparison of the performance with the conventional models.
표 3. 제안하는 모델과 기존 연구 모델들과의 성능 비교

Attack Type	Learning Method	Detection Model	Accuracy	Precision	Recall	F1-Score
DoS attack	Supervised	DCNN	99.97	100	99.89	99.95
	Semi-Supervised	CAAE	-	99.92	98.23	99.07
	Unsupervised	GIDS	97.90	96.80	99.60	98.18
		iForest	-	-	-	-
		NovelADS	-	99.97	99.91	99.94
		Our Model	99.28	99.37	99.61	99.49
Fuzzy attack	Supervised	DCNN	99.82	99.95	99.65	99.80
	Semi-Supervised	CAAE	-	99.99	84.26	91.45
	Unsupervised	GIDS	98.00	97.30	99.50	98.39
		iForest	99.29	95.07	99.93	97.44
		NovelADS	-	99.99	100	100
		Our Model	99.36	99.39	99.65	99.52
Gear attack	Supervised	DCNN	99.95	99.99	99.89	99.94
	Semi-Supervised	CAAE	-	99.77	99.78	99.77
	Unsupervised	GIDS	96.20	98.10	96.50	97.29
		iForest	99.24	94.79	100.00	97.33
		NovelADS	-	99.89	99.93	99.91
		Our Model	99.46	99.35	99.71	99.53
RPM attack	Supervised	DCNN	99.97	99.99	99.94	99.96
	Semi-Supervised	CAAE	-	99.84	99.55	99.70
	Unsupervised	GIDS	98.00	98.30	99.00	98.65
		iForest	99.85	98.97	100.00	99.48
		NovelADS	-	99.91	99.9	99.91
		Our Model	99.40	99.17	99.74	99.46

탐지 성능이 우수함을 알 수 있지만 지도학습 방식의 IDS라서 학습된 공격 유형만 탐지할 수 있다는 단점이 있다. CAAE 모델[19]는 준지도학습 기반으로 본 논문에서 제안하는 모델과 비교했을 때 전반적으로 성능이 비슷함을 알 수 있다. 하지만 CAAE 모델은 라벨링 된 공격 데이터를 힌트 데이터로 사용하기 때문에 비지도학습 모델과는 차이가 있다.

본 논문에서 제안하는 모델을 유사한 방식의 비지도학습 기반 IDS들과 비교한 결과는 다음과 같다. GAN을 이용하는 GIDS(GAN based Intrusion Detection System) 모델[8]과 비교했을 때, 본 논문에서 제안하는 모델이 모든 성능에서 우수하다는 것을 알 수 있다. 또한 iForest 모델을 이용한 IDS[9]와 비교했을 때, Recall 성능을 제외한 대부분의 성능 지표가 우수한 것을 확인할 수 있다. NovelADS 모델[10]은 본 논문에서 제안하는 모델에 비해 전반적으로 성능이 우수함을 확인할 수 있다. 하지만 해당 모델은 각각의 공격에 대해서 서로 다른 임계값을 사용함으로서, 어떤 공격이 발생할지 모르는 상황에서 임계값을 미리 특정 공격에 맞춰서 정해놓아야 한다는 단점이 있다. 이 점을 고려하였을 때, 하나의 임계값만을 사용한 본 논문의 모델이 다양한 공격 유형이 존재하는 환경에서 공격 탐지에 더 적절하다고 판단된다.

Ⅳ. 결론

본 논문에서는 오토인코더 모델과 가우시안 커널 밀도 추정 함수를 사용한 CAN 통신 침입 탐지 시스템을 제안

하였다. 오토인코더는 비지도학습 모델로 정상 데이터만을 학습하고 공격 데이터를 탐지할 수 있다. 따라서 지도학습 모델과는 다르게 알려지지 않은 공격을 탐지할 수 있다는 장점을 갖는다. 또한 가우시안 커널 밀도 추정 함수를 사용하여 4가지 공격 유형에 대하여 동일한 임계값을 가지며 모델이 정상 데이터와 공격 데이터를 잘 구분할 수 있는 최적의 프레임 개수를 구하였다. 이러한 최적의 임계값과 프레임 개수를 가지는 모델을 정상 데이터만을 학습시킨 후 4가지 다른 유형의 공격 데이터로 테스트를 진행하여 기존에 제안된 비지도학습 모델들보다 우수한 성능을 가짐을 보였다. 추후 연구로는 해당 모델을 하드웨어로 구현하고 실제 차량 환경에 적용하는 것을 목표로 한다.

References

[1] B. Bari, K. Yelamarthi, and S. Ghafoor, “Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study,” *Sensors*, vol.23, no.7, pp.3610, 2023. DOI: 10.3390/s23073610

[2] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, and S. Savage, “Experimental security analysis of a modern automobile,” *Proceedings of IEEE Symposium on Security and Privacy*, 2010. DOI: 10.1109/SP.2010.34

[3] A. Theissler, “Anomaly detection in recordings from in-vehicle networks,” *Proceedings of International Workshop on Big Data Applications and Principles*, 2014.

[4] A. Tomlinson, J. Bryans, and S. Shaikh, “Using a one-class compound classifier to detect in-vehicle network attacks,” *Proceedings of Genetic and Evolutionary Computation Conference*, 2018.
DOI: 10.1145/3205651.3208223

[5] D. Lee, C. Han, and S. Lee, “RIDS: Random Forest-Based Intrusion Detection System for In-Vehicle Network,” *Korean.electr.elctron.eng.*, vol.26, no.4, pp. 614, 2022.
DOI: 10.7471/ikeee.2022.26.4.614

[6] D. Lee, C. Han, and S. Lee, “Design and Implementation of Automotive Intrusion Detection System Using Ultra-Lightweight Convolutional Neural Network,” *Korean.electr.elctron.eng.,* vol.27, no.4, pp.524, 2023. DOI: 10.7471/ikeee.2023.27.4.524

[7] H. Song, J. Woo, and H. Kim, “In-vehicle network intrusion detection using deep convolutional neural network,” *Vehicular Communications,* vol.21, pp.100198, 2020.
DOI: 10.1016/j.vehcom.2019.100198

[8] E. Seo, H. Song, and H. Kim, “GIDS: GAN based intrusion detection system for in-vehicle network,” *Proceedings of. Annual Conference on Privacy, Security and Trust*, 2018.
DOI: 10.48550/arXiv.1907.07377

[9] P. Araujo-Filho, A. Pinheiro, G. Kaddoum, D. Campelo, and F. Soares, “An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks With a Low-Cost Platform,” *IEEE Access,* vol.9, pp.166855, 2021.
DOI: 10.1109/ACCESS.2021.3136147

[10] K. Agrawal, T. Alladi, A. Agrawal, V. Chamola, and A. Benslimane, “NovelADS: A Novel Anomaly Detection System for Intra-Vehicular Networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol.23, no.11, pp.22596, 2022.
DOI: 10.1109/TITS.2022.3146024

[11] F. Luo, J. Wang, X. Zhang, Y. Jiang, Z. Li, and C. Luo, “In-vehicle network intrusion detection systems: a systematic survey of deep learning-based approaches,” *PeerJ Computer Science*, vol.9, pp. 1648, 2023. DOI: 10.7717/peerj-cs.1648

[12] H. Alqahtani and G. Kumar, “A deep learning-based intrusion detection system for in-vehicle networks,” *Computers and Electrical Engineering*, vol.104, Part. B, pp.108447, 2022.
DOI: 10.1016/j.compeleceng.2022.108447

[13] J. Ashraf, A. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, “Novel Deep Learning-Enabled LSTM Autoencoder Architecture for Discovering Anomalous Events From Intelligent Transportation Systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol.22, no.7, pp.4507, 2021. DOI: 10.1109/TITS.2020.3017882

[14] S. Longari, D. Valcarcel, M. Zago, M. Carminati, and S. Zanero, “CANnolo: An Anomaly Detection

System Based on LSTM Autoencoders for Controller Area Network," *IEEE Transactions on Network and Service Management*, vol.18, no.2, pp.19134, 2021. DOI: 10.1109/TNSM.2020.3038991

[15] P. Cheng, M. Han, and G. Liu, "DESC-IDS: Towards an efficient real-time automotive intrusion detection system based on deep evolving stream clustering," *Future Generation Computer Systems*, vol.140, pp.266, 2023.
DOI: 10.1016/j.future.2022.10.020

[16] P. Wei, B. Wang X. Dai, L. Li, and F. He, "A novel intrusion detection model for the CAN bus packet of in-vehicle network based on attention mechanism and autoencoder," *Digital Communications and Networks*, vol.9, no.1, pp.14, 2023.
DOI: 10.1016/j.dcan.2022.04.021

[17] S. Lokman, A. Othman, S. Musa, and M. Bakar, "Deep contractive autoencoder-based anomaly detection for in-vehicle controller area network (CAN)," *Progress in Engineering Technology*, Springer Cham, 2019.
DOI: 10.1007/978-3-030-28505-0_16

[18] V. Kukkala, S. Thiruloga, and S. Pasricha, "INDRA: Intrusion Detection Using Recurrent Autoencoders in Automotive Embedded Systems," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol.39, no.11, pp.3698, 2020.
DOI: 10.1109/TCAD.2020.3012749

[19] T. Hoang and D. Kim, "Detecting in-vehicle intrusion via semi-supervised learning-based convolutional adversarial autoencoders," *Vehicular Communications*, vol.38, pp.100520, 2022.
DOI: 10.1016/j.vehcom.2022.100520

[20] Hacking and Countermeasure Research Lab, "Car-Hacking Dataset," https://ocslab.hksecurity.net/Datasets/car-hacking-dataset/

BIOGRAPHY

Donghyeon Kim (Member)

2023 : BS degree in Electronic Engineering, Soongsil University.
2023~ : Candidate for MS degree in the Department of Intelligent Semiconductors, Soongsil University.
〈Main Interest〉 Vehicle Security, Artificial Intelligence, Accelerator, Automotive SoC

Hyungchul Im (Member)

2021 : BS degree in Mechanical Engineering, Soongsil University.
2021~ : Candidate for Ph.D degree in Electronic Engineering, Soongsil University.
〈Main Interest〉 Vehicle Security, Artificial Intelligence, Automotive SoC

Seongsoo Lee (Life Member)

1991 : BS degree in Electronic Engineering, Seoul National University.
1993 : MS degree in Electronic Engineering, Seoul National University.
1998 : PhD degree in Electrical Engineering, Seoul National University.
1998~2000 : Research Associate, University of Tokyo.
2000~2002 : Research Professor, Ewha Womans University.
2002~Now : Professor in School of Electronic Engineering, Soongsil University.
〈Main Interest〉 AI SoC, Automotive SoC, Security SoC, Processor SoC, Power Management SoC, Battery Management SoC, Reliability and Safety.