ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
j.inst.Korean.electr.electron.eng.Vol.27,No.4,531~536,December 2023
논문번호 23-04-23
https : //doi.org/10.7471/ikeee.2023.27.4.531
164

차량용 경량화 침입 탐지 시스템을 위한 데이터 전처리 기법

Data Preprocessing Method for Lightweight Automotive Intrusion Detection System

박 상 민*, 임 형 철*, 이 성 수*★

Sangmin Park*, Hyungchul Im*, and Seongsoo Lee*★

Abstract

This paper proposes a sliding window method with frame feature insertion for immediate attack detection on in-vehicle networks. This method guarantees real-time attack detection by labeling based on the attack status of the current frame. Experiments show that the proposed method improves detection performance by giving more weight to the current frame in CNN computation. The proposed model was designed based on a lightweight LeNet-5 architecture and it achieves 100% detection for DoS attacks. Additionally, by comparing the complexity with conventional models, the proposed model has been proven to be more suitable for resource-constrained devices like ECUs.

요 약

본 논문에서는 차량 내 네트워크에서 즉각적인 공격 탐지를 위해 프레임 피처 삽입이 적용된 슬라이딩 윈도우 기법을 제안한다. 이 방법은 현재 프레임의 공격 여부에 따라 라벨링을 진행하기 때문에 공격 탐지의 실시간성을 보장할 수 있다. 또한 이 방법이 CNN 연산에서 현재 프레임에 대한 가중치를 주어 성능을 향상시킬 수 있음을 실험을 통해 확인하였다. 제안하는 모델은 경량화된 LeNet-5 구조 기반으로 설계되었으며 DoS 공격 탐지 성능에서 100%를 달성하였다. 또한 기존 연구의 모델들과 복잡성을 비교했을 때 제안하는 모델이 ECU와 같이 리소스가 제한된 장치에 더 적합함을 확인하였다.

Key words : Controller Area Network, Intrusion Detection System, Sliding Window, Frame Feature Insertion, Data preprocessing, Convolutional Neural Network, LeNet-5

* 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). (20023805, RS-2022-00155731, RS-2022-00232192)
Manuscript received Dec. 14, 2023; revised Dec. 20, 2023; accepted Dec. 21, 2023.

Ⅰ. 서론

자율 주행 기술의 발전에 따라 차량 내 네트워크(IVN: In-Vehicle Network)에서 보안의 중요성이 증가하고 있다. CAN 버스[1]는 차량 내의 ECU(Electronic Control Unit)끼리 데이터를 통신하고 시스템을 제어할 수 있게 해준다. 그러나 CAN 버스는 별도의 보안 기술이 적용되지 않아 하나의 ECU가 해킹되는 경우 차량 제어에 심각한 문제가 발생하며 심한 경우 안전 운행이 불가능해질 수도 있다. 따라서 CAN 버스의 보안 취약성을 보완하기 위하여 침입 탐지 시스템(IDS: Intrusion Detection System)이 필요하며, 최근 많은 연구가 이루어지고 있다.

침입 탐지 시스템은 대부분 CNN(Convolutional Neural Network)[2]과 같은 인공지능 기술을 사용하는데 여기에서 전처리(Preprocessing)는 CNN의 성능에 큰 영향을 미치는 단계이다. 따라서 차량용 침입 탐지 시스템[3]-[5]에 적합하고 성능이 우수한 전처리 기법을 개발할 필요가 있다. 전처리 단계에서는 CAN 프레임을 그룹으로 묶어서 처리하는데, 기존의 전처리 기법은 대부분 공격이 이루어지는 CAN 프레임을 특정하지 않기 때문에 여러 개의 CAN 프레임이 묶인 그룹별로는 공격을 탐지할 수 있지만 그 그룹 내에 어떤 CAN 프레임이 공격인지는 탐지할 수 없다는 단점을 가지고 있다.

이를 보완하기 위하여 Transformer-Based Attention Network를 이용하는 침입 탐지 시스템이 제안되었다[6]. 하지만 이 기법은 복잡도가 크기 때문에 컴퓨팅 용량이 제한되어 있는 ECU에 적용하기 어렵다는 단점이 존재한다[7]. [8]에서는 경량화된 CanNet을 제안하고 차량 내 DoS 공격을 효과적으로 탐지할 수 있는 방안을 제안하였다.

본 논문에서는 실시간으로 프레임별 공격 탐지가 가능한 효과적인 데이터 전처리 기법을 제안한다. 제안하는 방법은 프레임 삽입이 적용된 슬라이딩 윈도우 기법으로 실시간으로 공격을 탐지할 수 있을 뿐만 아니라, CNN 연산 시 현재 프레임에 가중치를 주어 성능을 향상시킬 수 있다. 또한 경량화 LeNet-5 기반 모델을 제안하여 리소스가 제한된 장치에 적합함을 나타낸다.

Ⅱ. CAN 통신 및 공격 유형

1. CAN 통신

CAN은 실시간 메시지 전송을 보장할 뿐만 아니라 2선 차동 신호를 사용하여 노이즈에 매우 강하고, 에러 검출 및 오류 회복, 재전송 기능을 통한 고신뢰성을 지닌 자동차의 ECU 간 통신을 위한 표준 프로토콜이다. 또한 CAN 통신은 버스 시스템을 통하여 데이터를 효율적으로 전송하며, 멀티 마스터 구조로 언제든지 통신을 시작할 수 있다는 장점을 갖는다. 하지만 다중 마스터 통신 특성으로 인해 여러 노드가 동시에 송신을 시작하면 중재 메커니즘(Arbitration mechanism)에 따라 CAN 프레임 중 11비트 ID(Identifier)를 우선 순위로 하여 우선순위가 낮은 노드부터 송신에서 탈락하고 최종적으로 가장 우선 순위가 높은 노드가 이후 송신을 계속한다. 이때 송신에서 탈락한 다른 노드들은 수신 모드로 전환하여 다음 번 송신을 기다린다.

2. CAN 버스 공격 유형

본 논문에서는 DoS 공격, Spoofing 공격, Fuzzy 공격에 대해 다룬다. 먼저, DoS 공격은 공격자가 단일 노드에서 CAN 버스에 우선순위가 높은 데이터를 지속적으로 송신하여 통신이 정상적으로 동작하지 못하도록 방해하는 공격이다. 예를 들어 ID가 0x000인 CAN 프레임을 연속적으로 송신함으로써 정상적인 노드들의 송수신을 방해한다.

Spoofing 공격은 공격자가 일정기간 CAN 트래픽을 분석한 뒤, 특정 장치와 연관된 ID를 파악하고 특정 장치에 오작동을 일으키는 메시지를 송신하는 공격이다. 예를 들어 공격자는 특정 ECU의 RPM 또는 Gear와 관련된 CAN 프레임을 분석하고, 해당 장치를 임의로 조작하여 차량 주행을 방해할 수 있다.

Fuzzy 공격은 공격자가 CAN 버스에 무작위로 생성한 데이터를 송신하는 공격이다. 무작위의 CAN ID와 데이터를 CAN 버스에 주입함으로써 정상 노드들의 데이터 전송을 지연시키거나, 차량 내 시스템에 오동작을 유발할 수 있다.

Ⅲ. 경량화 침입 탐지 시스템

1. 제안하는 전처리 기법

본 논문에서는 프레임 단위로 공격 여부를 탐지하기 위해 프레임 삽입이 적용된 슬라이딩 윈도우 기법을 제안한다. 프레임 삽입이 적용되지 않은 일반적인 슬라이딩 윈도우 기법은 그림 1에 나타내었다. 먼저, CAN ID 이미지를 생성하기 위해서 연속된 11개의 CAN 프레임에서 ID만을 추출한다. 생성된 이미지는 CAN ID 11비트와 11개의 프레임으로 이루어진 11×11 바이너리 이

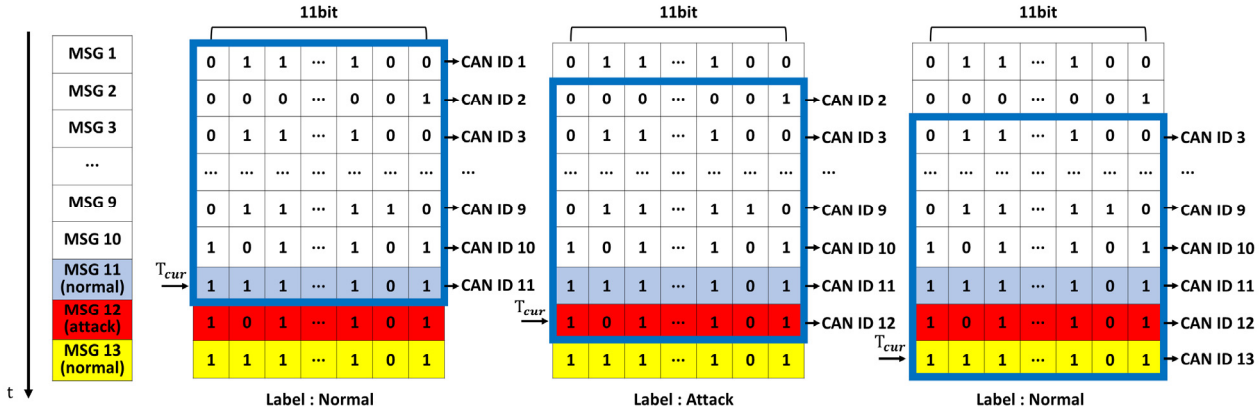

Fig. 1. Conventional sliding window method.
그림 1. 일반적인 슬라이딩 윈도우 기법

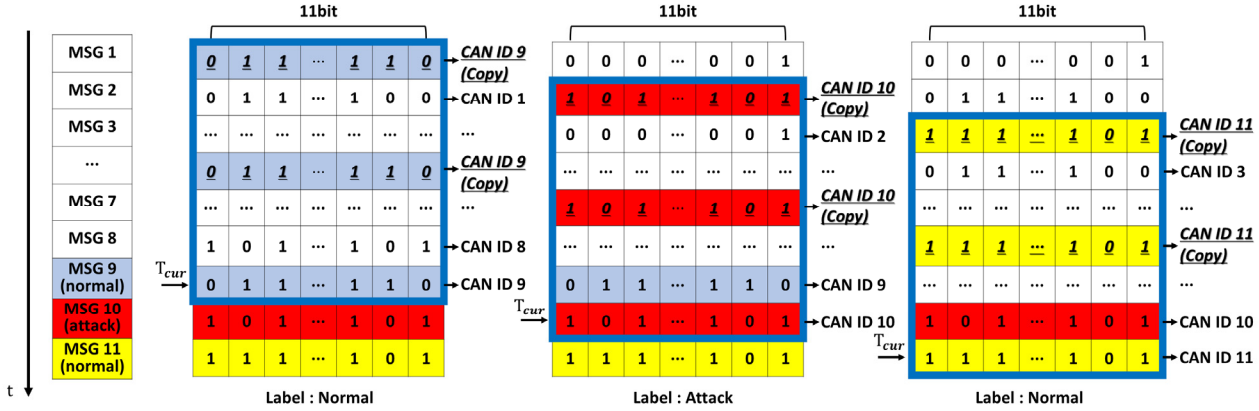

Fig. 2. Proposed sliding window method.
그림 2. 제안하는 슬라이딩 윈도우 기법

미지를 나타낸다. 이때, 윈도우 스트라이드를 1로 설정하여 한 프레임별로 라벨링을 진행하게 된다. 따라서 마지막 시퀀스에 위치한 ID를 현재 수신한 프레임이라고 가정하고, 현재 프레임의 공격 여부에 따라 라벨링을 진행한다. 이와 같은 방법으로 학습을 진행하게 되면 현재 수신한 프레임을 기준으로 공격 여부를 판단하기 때문에 실시간성을 보장할 수 있다.

CNN 연산은 11×11 바이너리 이미지 전체에 대하여 동일하게 합성곱을 진행하게 된다. 그러나 CNN 연산의 이러한 특성 때문에, 현재 수신된 프레임(마지막 프레임)을 기준으로 라벨링하는 전처리 방법으로는 가장 중요한 정보인 현재 수신 프레임(마지막 프레임)이 다른 프레임과 동일한 가중치로 처리되기 때문에 성능이 저하될 수 있다. 이러한 문제를 해결하기 위해 본 논문에서는 그림 2와 같은 방법으로 현재 수신된 프레임에 가중치를 더 부여하였다. 먼저 11개 프레임의 ID가 아닌 9개의 프레임 ID를 추출하고, 마지막 프레임의 ID를 바이너리 이미지의 상단 및 중단에 복사하여 삽입한다. 즉, 1~11번 ID 대신에 1~9번 ID를 사용하되, 마지막 ID인 9번을 상단, 중단에 중복 삽입하여 9, 1, 2, 3, 4, 9, 5, 6, 7, 8, 9번의 11개 ID를 사용한다. 이와 같은 방법은 CNN 연산 시 다른 프레임보다 마지막 프레임에 더 많은 가중치를 주어 모델의 성능을 향상시킬 수 있다. 성능 향상을 보여주기 위해 Fuzzy 공격에 대한 결과를 표 1에 나타내었다.

Table 1. Performance comparison of frame feature insertion.
표 1. 프레임 피처 삽입의 성능 비교

	Sliding Window (with Insertion)	Sliding Window (without Insertion)
Accuracy	0.9906	0.9460
Precision	0.9521	0.8262
Recall	0.9792	0.7554
F1 Score	0.9549	0.7892

2. LeNet-5 기반 경량화 IDS 모델

본 논문에서 사용한 LeNet-5 기반의 경량화 모델을 그림 3과 표 2를 통하여 나타내었다. 제안하는 모델은 프레임 삽입이 적용된 슬라이딩 윈도우 기법을 통해 생성한 11×11의 이미지를 입력받아 제로 패딩을 진행한다. 또한 3×3 크기를 가진 필터 16개로 컨볼루션 연산을 진행한다. 또한 첫 번째 컨볼루션 연산 결과를 스트라이드를 2로 설정한 2×2 사이즈의 맥스 풀링을 진행한다. 두 번째 컨볼루션에서는 필터 32개를 사용하여 연산을 진행한다. 이때 동일하게 제로 패딩을 추가하고, 맥스 풀링을 통해 2×2 출력 모양 32개가 만들어진다. 이 결과를 Flatten 과정을 통해 1차원 데이터로 변환한다. 마지막으로 2개의 dense 층을 지나 활성화 함수인 Sigmoid를 통해 공격과 정상 데이터로 분류하는 학습이 진행된다. 학습은 Learning Rate 0.001을 사용하였고, epoch 10에 대하여 Nadam을 optimizer로 사용하였다.

Table 2. Structure of reduced LeNet-5.
표 2. 경량화 LeNet-5의 구조

Layer	Filter shape	Output	Parameters
Conv 1	16×3×3	16×11×11	160
Max Pool 1	2×2	16×5×5	64
Conv 2	32×3×3	32×5×5	4640
Max Pool 2	2×2	32×2×2	128
Fully Connected	64	64	8256
Classification	1	1	65

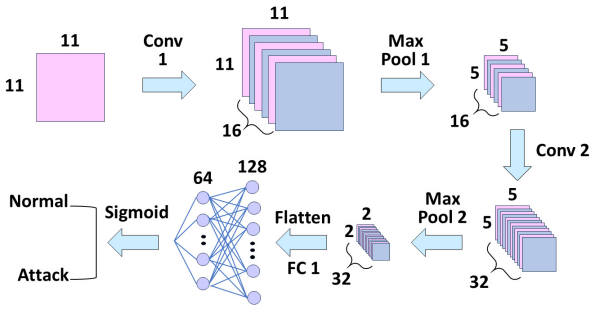

Fig. 3. Structure of the reduced LeNet-5.
그림 3. 경량화 LeNet-5 구조

Ⅳ. 실험 결과

본 논문에서 사용된 차량 해킹 데이터 세트[9]는 DoS 공격, Gear 및 RPM spoofing 공격, fuzzy 공격 등 4가지 공격 데이터 세트로 구성되어 있다. 각 공격 데이터 세트는 훈련용 70%, 테스트용 30%로 나누어 사용되었다.

DoS 공격에 대한 성능을 기존에 제안된 모델들과의 비교를 표 3에 나타내었다. 먼저, DCNN[4]을 이용한 모델은 앞서 설명한 바와 같이 29 프레임 단위로 공격을 판단한다. 즉 29 프레임 중에 공격이 하나 이상 포함되었을 경우 공격으로 라벨링 되었기 때문에 정확히 어떤 프레임이 공격인지 확인할 수 없다. GIDS[5]의 경우, GAN을 이용한 비지도학습 모델로 학습에 사용되지 않은 공격을 탐지할 수 있다는 장점이 있다. 하지만 64 프레임 단위로 공격 여부를 판단하기 때문에 [4]에서와 같은 문제점을 갖는다. 마지막으로 리소스가 제한되어있는 차량용에 적용하기 위한 DoS 공격 탐지 모델인 CanNet[8]이 제안되었다. 또한 [8]에서는 공격 시간을 추적하는 방안을 제안하여 어떤 프레임이 공격인지 알 수 있다. 하지만 공격 시간을 추적하기 위해 모든 시간을 기록해야 한다는 문제점이 존재한다.

Table 3. Performance comparison of detection methods.
표 3. 탐지 방법에 따른 성능 비교

Index	DCNN[4]	GIDS[5]	CanNet[8]	Reduced LeNet-5 (proposed)
Parameters	1.615M	1.52M	23.70K	13.3K
FLOPs	104.1M	1.59M	1.64M	143.7K
Accuracy	0.9963	0.9790	0.9976	1.0
Precision	0.9989	0.9680	0.9981	1.0
Recall	0.9971	0.9960	0.9977	1.0
AUC	0.999	0.999	0.999	1.0

Table 4. Performance comparison of attack types.
표 4. 공격 유형별 성능 비교

Attack	Accuracy	Precision	Recall	F1 Score
DoS	1.0	1.0	1.0	1.0
RPM	0.9927	0.9956	0.9750	0.9852
Gear	0.9767	0.9722	0.9049	0.9373
Fuzzy	0.9916	0.9517	0.9950	0.9728

본 논문에서 제안하는 모델은 DoS 공격을 성공적으로 탐지하는 것을 실험 결과를 통해 확인할 수 있다. 또한 슬라이딩 윈도우 기법을 통하여 라벨링 되었기 때문에 어떤 프레임이 공격인지 명확하게 알 수 있다. 마지막으로 제안하는 모델은 다른 모델들에 비해 적은 파라미터와 FLOPs를 나타낸다. 이는 하드웨어 구현에 유리하며

ECU와 같이 리소스가 제한되어 있는 디바이스에 제안하는 모델을 적용하기에 더 효율적임을 알 수 있다. 하지만 DoS 공격이 아닌 다른 공격 유형들에 대해서는 비교적 낮은 성능을 나타내는 것을 표 4를 통해 알 수 있다. 이는 작고 단순한 모델을 사용했기 때문에 DoS 공격보다 패턴이 복잡한 공격 유형들의 특징을 잘 추출하지 못했기 때문이다.

Ⅴ. 결론

본 논문에서는 CAN 통신에서 즉각적인 공격 여부를 판단할 수 있는 데이터 전처리 방안을 제안하였다. 또한, LeNet-5를 기반으로 한 경량화된 CNN 모델을 제안하였다. 제안한 방법과 모델을 통해 DoS 공격을 100% 탐지할 수 있음을 확인하였다. 또한 제안하는 모델이 기존에 제안된 모델들에 비해 현저히 낮은 복잡도를 갖기 때문에 리소스가 제한된 장치에 적합함을 알 수 있다.

References

[1] ISO 11898-1:2015, “Road Vehicles-Controller Area Network (CAN)-Part 1: Data Link Layer and Physical Signaling,” https://www.iso.org/standard/63648.html

[2] An Introduction to Convolutional Neural Networks (CNNs), https://www.datacamp.com/tutorial/introduction-to-convolutional-neural-networks-cnns

[3] S. Woo, H. J. Jo, and D. H. Lee, “A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN,” *IEEE Transactions on Intelligent Transportation Systems,* vol.16, no.2, pp.993-1006, 2015.
DOI: 10.1109/TITS.2014.2351612

[4] H. Song, J. Woo, and H. Kim, “In-Vehicle Network Intrusion Detection Using Deep Convolutional Neural Network”, *Vehicular Communications,* vol.21, pp.1-13, 2020.
DOI: 10.1016/j.vehcom.2019.100198

[5] E. Seo, H. Song, and H. Kim, “GIDS: GAN Based Intrusion Detection System for In-vehicle Network,” P*roceedings of Annual Conference on Privacy, Security and Trust,* pp.1-6, 2018.
DOI: 10.1109/PST.2018.8514157

[6] T. Nguyen, H. Nam, and D. Kim, “Transformer-Based Attention Network for In-Vehicle Intrusion Detection,” *IEEE Access,* pp.55389-55403, 2023.
DOI: 10.1109/ACCESS.2023.3282110

[7] Y. Abadade, A. Temouden, H. Bamoumen, N. Benamar, Y. Chtouki, and A. Hafid, “A Comprehensive Survey on TinyML,” *IEEE Access,* pp.96892-96922, 2023. DOI: 10.1109/ACCESS.2023.3294111

[8] S. Gao, L. Zhang, L. He, X. Deng, H. Yin, and H. Zhang, “Attack Detection for Intelligent Vehicles via CAN-Bus: A Lightweight Image Network Approach,” *IEEE Transactions on Vehicular Technology,* pp.1-13, 2023. DOI: 10.1109/TVT.2023.3296705

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

BIOGRAPHY

Sangmin Park (Member)

2018~ : Candidate for BS degree in Electronic Engineering, Soongsil University
〈Main Interest〉 Vehicle Security, Artificial Intelligence, 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