

소프트웨어 정의 공장의 비트스트림 기반 반도체 생산 프로토콜 분류 자동화 프레임워크에 대한 연구

A Study on Bit String-Based Semiconductor Manufacturing Protocol Classification for Software-Defined Factory

구남영

fantage9@gmail.com

June, 2026



중앙대학교
CHUNG-ANG UNIVERSITY



본 발표자료 중 일부 그림은 생성 AI를 활용하여 제작되었습니다

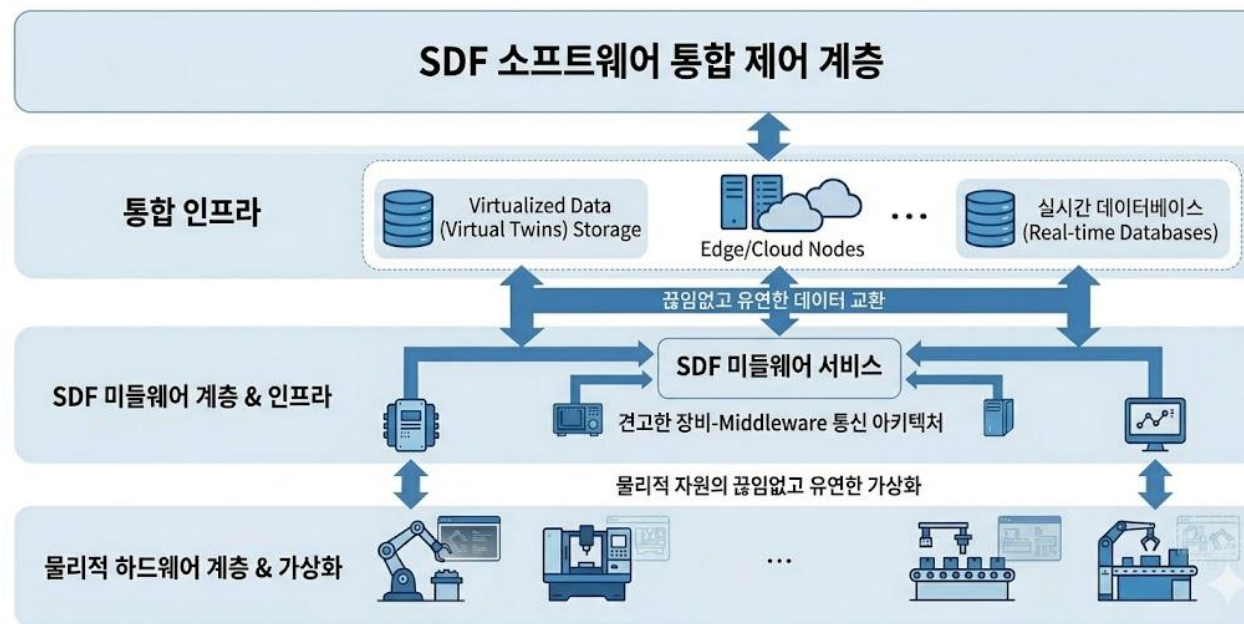
Contents

- 1. Introduction**
- 2. Related Work**
- 3. Proposed Framework**
- 4. Experimental Settings**
- 5. Overall Experimental Results**
- 6. In-Depth Analysis**
- 7. Conclusion**

Introduction

Software-Defined Factory (SDF)

- 현대의 제조 산업은 Industry 5.0을 향해 가고 있으며, 이를 구현하기 위해 공장 내의 모든 물리적 자원을 가상화하고 소프트웨어 기반으로 통합 제어하는 소프트웨어 정의 공장(Software-Defined Factory, SDF)이 대두되고 있음 [1-4].
- SDF는 크게 Hardware Layer와 Infrastructure Layer로 구분되는데, SDF가 온전하게 기능하기 위해서는 이 두 Layer간의 끊임없고 유연한 데이터 교환이 필수적이며, 이를 위해 장비-미들웨어(Middleware) 간의 견고한 통신 아키텍처가 구축되어야 함 [5-6].

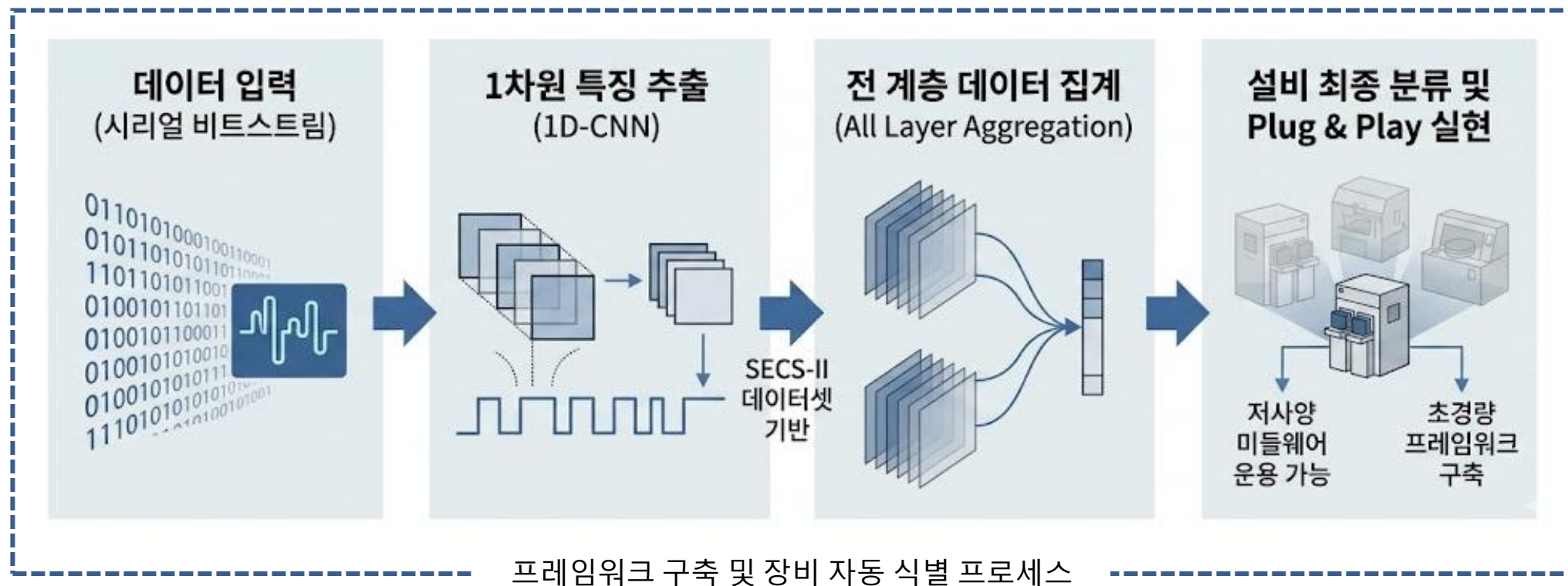


- [1] Zhong, R. Y., Xu, X., Klotz, E., and Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: a review. *Engineering*, 3(5):616–630.
- [2] Kim, J., Lee, J., Park, S. J., Lee, J., Song, B., and Moon, S. K. (2025). Software-defined factory: Paradigm shift in manufacturing towards industry 5.0. *International Journal of Precision Engineering and Manufacturing-Smart Technology*, 3(2):201–209.
- [3] Ahn, J., Yun, S., Kwon, J.-W., and Kim, W.-T. (2024). Literacy deep reinforcement learning-based federated digital twin scheduling for the software-defined factory. *Electronics*, 13(22):4452.
- [4] Koyasako, Y., Suzuki, T., Hatano, T., Shimada, T., and Yoshida, T. (2024). Demonstration of industrial ethernet protocol softwareization and advanced motion control for full software-defined factory network. *IEEE Access*, 12:104020–104030.
- [5] Iwao, T. (2018). Architecture of semiconductor equipment networks. *IEEE Transactions on Semiconductor Manufacturing*, 31(2):241–247.
- [6] Moyne, J. and Iskandar, J. (2017). Big data analytics for smart manufacturing. *Processes*, 5(3):39.

Introduction

Objective and Procedure

- 본 연구의 목적은 시리얼 비트 시퀀스만으로 연결된 장비를 자동으로 식별하여 Plug & Play 환경을 조성하며, 저사양 미들웨어 장비에서도 운용 가능한 초경량 통신 프레임워크를 구축하는 것임.
- 반도체 장비 시나리오 기반 SECS-II 비트스트림(Bitstream) 데이터셋을 구축하고, 여기에서 1차원 합성곱 신경망(1D-CNN) 기반 특징을 추출한 다음 전 계층 집계(All Layer Aggregation) 모델을 적용하여 장비를 분류함.



Introduction

Problem and Strategy

- 순수 시리얼 통신을 고집하며 식별 정보가 전무한 레거시(Legacy) 반도체 장비들을 공장에 도입하게 될 경우, 엔지니어가 수동으로 파라미터들을 프로그래밍하고 설정해야 하므로 많은 과부하와 병목 현상이 발생하고 있음.
- 본 연구는 물리적 통신 비트스트림을 0/1 시계열 신호로 간주하여, 복잡한 프로토콜 역공학(Protocol Reverse Engineering, PRE)과 같은 방식 대신 효율적인 다중 클래스 분류 문제로 관점을 치환하여 해결하고자 함.



파라미터 수동 설정
Manual Programming

과부하 및 병목
Overload & Bottleneck, [23]

현재 상태



비트스트림 시계열 활용
Bitstream Utilization

다중 클래스 자동 분류
Auto Multi-class Classification

제안 전략

Related Work

Protocol Reverse Engineering (PRE)

- 명세서가 유실된 레거시 시스템이나 사설 Protocol의 메시지 포맷을 자동으로 복원하기 위한 프로토콜 역공학은 기계학습의 발전과 함께 새로운 국면을 맞이하고 있음 [7].
- 초기 PRE 연구들은 통계적/휴리스틱 기법에 의존하였고 [8], 2024년 이후 딥러닝과 자연어 처리(NLP)를 융합한 연구가 많아지고 있으며 [9], 최근에는 데이터를 Character와 Sentence로 간주하여 언어 모델에 학습시키는 접근법이 각광받고 있음 [10-12]

구분	주요 시기	분석 기법 및 특징	대표 도구 및 기술	장점	단점 및 한계
1~3세대 (통계 및 휴리스틱 기반)	1990 ~ 2010 후반	전문가 지식(휴리스틱)과 통계적 모델의 결합 - 패킷 페이로드의 통계적 특성(빈도, N-gram 등) 분석 - 특정 규칙을 찾기 위한 서열 정렬 및 휴리스틱 기반 패턴 매칭 - 프로그램 메모리를 추적하여 포맷을 역산하는 휴리스틱 바이너리 분석(동적 오염 분석 등)	Wireshark, Netzob, Polyglot, Dispatcher 등	전문가의 직관을 반영하여 비암호화 환경에서 특정 프로토콜에 맞춘 빠른 분석 및 포맷 추론 가능	복잡한 암호화/압축 프로토콜에 취약하며, 변종 등장 시 매번 새로운 통계 모델이나 휴리스틱 룰 업데이트(전문가 개입) 필요
4세대 (머신러닝/딥러닝 기반)	2010 후반 ~ 2020 초	AI를 활용한 패턴 및 상태 추론 - NLP(자연어처리) 기법, RNN/LSTM, 클러스터링 알고리즘을 패킷 시퀀스에 적용 - 딥러닝을 통한 네트워크 상태 머신(State Machine) 추출	NEMESYS, WASP, 머신러닝 기반 클러스터링 프레임워크	대규모 데이터 처리에 용이, 새로운 변종 프로토콜에 대한 유연한 대처 및 높은 확장성	모델 학습을 위한 방대한 데이터 필요, 결과에 대한 해석 가능성(Interpretability)이 떨어짐
5세대 (LLM 및 하이브리드)	2020 중반 ~ 현재	LLM 기반 의미론적 분석 및 융합 - 대규모 언어 모델을 활용하여 RFC 문서와 트래픽 데이터 간의 연관성 분석 - 바이너리 기호 실행과 AI 추론을 결합한 하이브리드 접근법	GPT-4 등 LLM을 활용한 자동화된 퍼저(Fuzzer) 연동 시스템, 최신 AI 융합 프레임워크	사람 수준의 문맥 이해 및 '의미(Semantics)' 파악 가능, 퍼징(Fuzzing) 등 후속 보안 테스트와 즉각적 연동	AI의 환각(Hallucination) 오류 가능성, 컨텍스트 토큰 한계, 실시간 분석의 어려움

[7] Wang, Y. et al. (2024). Deep learning for unknown protocol reverse engineering: Challenges and opportunities. IEEE Network.

[8] Bossert, G., Guhier, F., and Hiet, G. (2014). Netzob: Inference of reverse-engineered communication protocols. IEEE Security and Privacy.

[9] Ghimire, A. et al. (2025). A survey on application of ai on reverse engineering for software analysis and security. IEEE Access

[10] Wei, X., Dai, H., Wang, Y., Shi, T., Sun, B., and Sun, J. (2026). A deep learning framework for industrial control protocol reverse engineering with multi-view attention and contrastive feature enhancement. Engineering Letters, 34(3):993–1000.

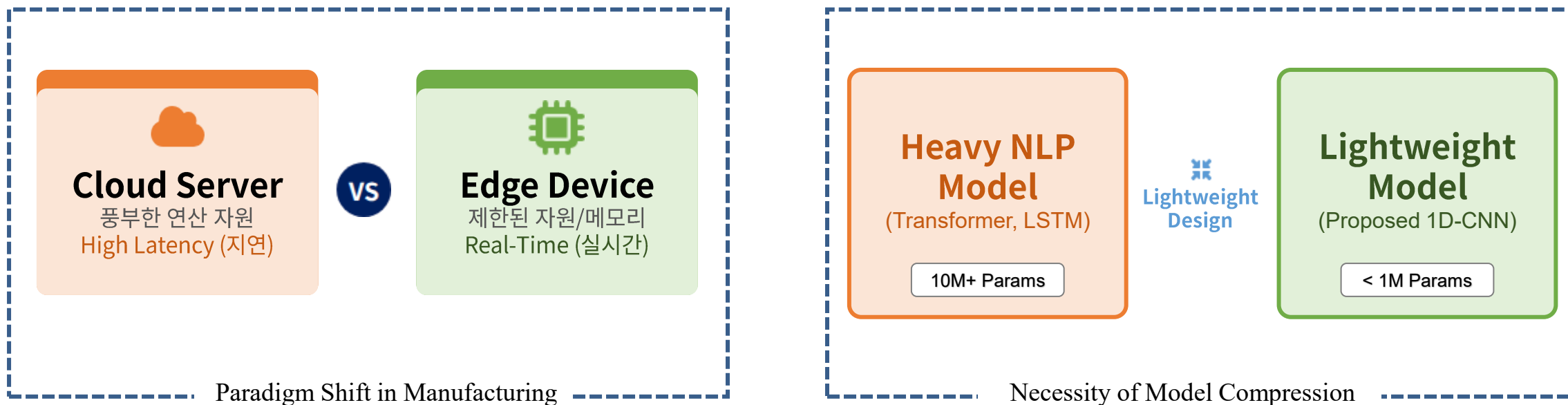
[11] Chen, L. et al. (2025). Transre: Transfer learning based protocol reverse engineering using self-attention. Journal of Network and Computer Applications

[12] Meng, X. et al. (2024). Protocolgpt: Prompting large language models for network protocol understanding. In Proceedings of the 33rd USENIX Security Symposium.

Related Work

소프트웨어 정의 공장을 위한 신경망 요구사항

- 산업 현장의 실시간 제어를 위해 클라우드 서버를 거치지 않고 단말 장치(Edge)에서 직접 데이터를 분석하여 지연 시간을 최소화하는 엣지 컴퓨팅 기술이 차세대 소프트웨어 정의 공장(SDF)의 필수 요소로 자리잡고 있음.
- 그러나 엣지 디바이스는 연산 자원과 메모리가 매우 제한적이므로 무거운 기존 딥러닝 모델을 탑재할 수 없어, 정확도 손실을 최소화하면서 파라미터와 연산량을 극단적으로 줄이는 신경망 경량화(Lightweighting)가 필수적임 [14].

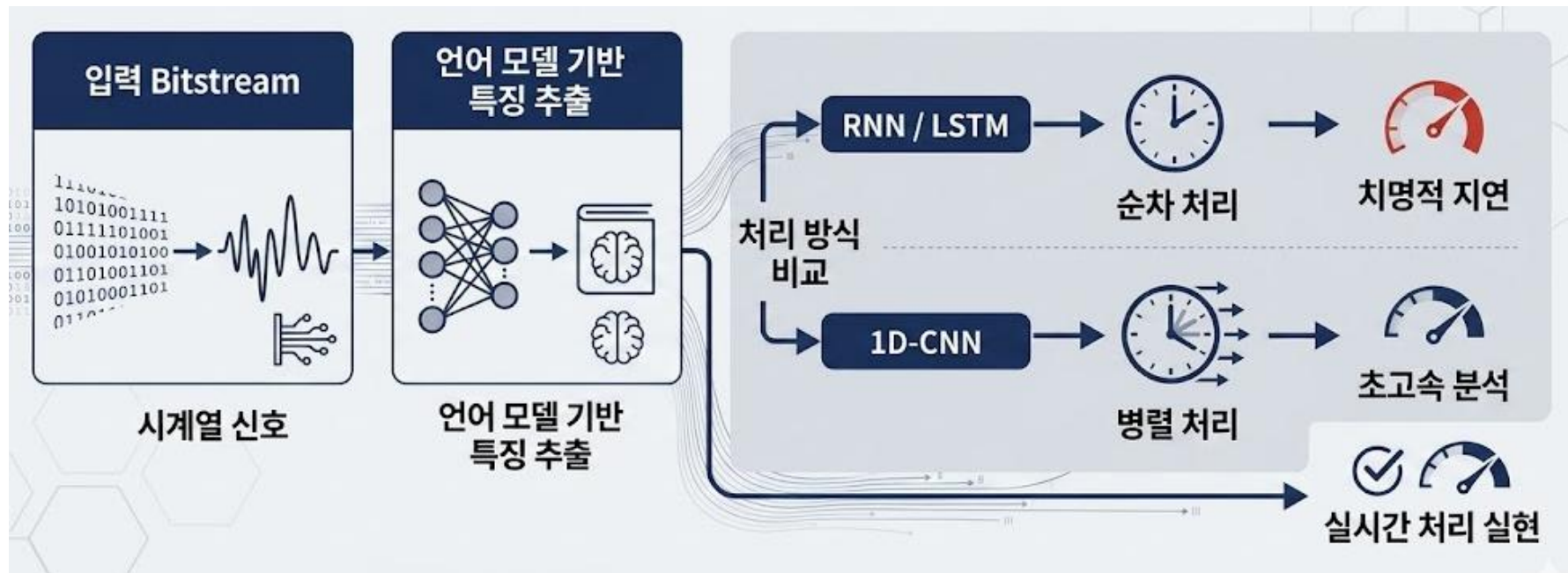


[14] Park, J., Kim, D.-W., and Lee, J. (2024). Calanet: Cheap all-layer aggregation for human activity recognition. In Advances in Neural Information Processing Systems (NeurIPS).

Related Work

경량 신경망 기반 비트스트림 분류

- Bitstream을 0과 1로 구성된 시계열 신호로 간주하여 신경망 모형에 학습시키면, 데이터에 내재된 프로토콜 규칙과 장비의 고유한 특징들을 효과적으로 추출할 수 있음.
- 또한 기존 순환 신경망(RNN)이나 장단기 기억망(LSTM)이 가진 치명적인 추론 지연 한계를 극복하기 위해, 병렬 연산을 통해 지역적 패턴을 초고속으로 파악할 수 있는 1차원 합성곱 신경망(1D-CNN)이 실시간 분석을 위한 대안이 될 수 있음 [13].



[13] Fawaz, H. I., Forestier, G., Weber, J., Idoumghar, L., and Muller, P.-A. (2019). Deep learning for time series classification: a review. Data mining and knowledge discovery, 33(4):917–963.

Common Drawback of Conventional Methods

- 대규모 언어 모델(LLM) 기반의 프로토콜 역공학 기법들은 복잡한 구조를 완벽하게 복원하는 데는 탁월하지만, 시퀀스 길이가 길어질수록 연산량이 기하급수적으로 증가하여 막대한 컴퓨팅 자원을 소모한다는 치명적인 단점을 지니고 있음.
- 따라서 컴퓨팅 자원이 제한된 엣지 디바이스 환경에서 방대한 시리얼 비트스트림을 즉각적으로 처리하기에는 연산 부하가 너무 커서, 실제 산업 현장에서 필수적인 실시간성(Real-time capability)을 전혀 보장할 수 없다는 것이 공통적인 한계임.

Algorithm	Author, year	Journal / Conference	Summary	Drawback
Deep Learning PRE	Wang, Y (2024)	IEEE Network	기계학습 및 딥러닝을 도입하여 미지의 통신 프로토콜 구조와 메시지 포맷을 자동으로 복원하는 역공학 연구 동향 제시	마스터-슬레이브 엣지 컴퓨팅 환경에 적용하기에는 컴퓨팅 자원이 막대하게 소모됨
ProtocolGPT	Meng, X (2024)	USENIX Security Symposium	대규모 언어 모델(LLM)에 프롬프트를 주입하여 프로토콜의 유한 상태 기계(FSM) 자체를 생성해 내는 생성형 추론 모델	수십억 개의 파라미터를 동원하므로 컴퓨팅 부하가 극심하여 산업용 현장 적용성이 매우 떨어짐
CALANet	Park, J (2024)	NeurIPS	네트워크 내 모든 계층의 특징 맵을 글로벌 풀링으로 압축하고 저비용으로 결합하여 파라미터를 최소화하는 초경량 네트워크	사용자 행동 인식(HAR) 도메인에 맞춰 고안되어, 시리얼 비트스트림 분류 도메인 적용을 위해 발상의 전환과 최적화가 필요함
BiLSTM + Self-Attention	Wei, X (2026)	Engineering Letters	통신 필드의 장거리 의존성을 포착하는 자기 주의 메커니즘과 조건부 무작위장(CRF)을 결합하여 상태 기계를 추론하는 프레임워크	시퀀스 길이 L 에 대해 $O(L^2)$ 의 연산량을 요구하여, 수 밀리초 이내에 추론해야 하는 임베디드 환경에 부적합함

Proposed Framework

Notation and Definition

- 1차원 합성곱 신경망(1D-CNN)은 비트스트림의 미시적 및 거시적 패턴을 추출하기 위해 수학적 연산을 수행하며, 이 과정에서 사용되는 핵심 텐서(Tensor)와 파라미터 기호들에 대한 명확한 정의는 네트워크 구조 이해를 위한 필수적 기반임.
- 특히 연산 자원의 한계를 극복하기 위해 설계된 전 계층 집계(All-Layer Aggregation) 메커니즘을 구체화하기 위해, 특징 맵의 차원 압축부터 최종 장비 분류 확률 도출에 이르는 데이터 흐름의 주요 표기법을 아래와 같이 정리하였음.

Symbol	Name of Symbol	Explain
$W_{j,i}^{(l)}(k)$	Convolutional Kernel (Weight)	신경망이 학습하는 필터 가중치 행렬. 특정 제어 비트(Start/Parity) 패턴을 스캐닝하는 역할
K	Kernel Size	필터의 크기 (본 논문에서는 연속된 프레임을 포괄하기 위해 홀수인 5 또는 7을 사용)
s	Stride	필터가 비트스트림 위를 이동할 때 한 번에 건너뛰는 간격 (슬라이딩 간격)
C_{l-1}	Input Channels	이전 계층($l - 1$)에서 전달받은 특징 맵의 채널 개수
$b_j^{(l)}$	Bias (편향)	특징 맵의 출력 값을 세밀하게 조정하기 위해 더해지는 학습 가능한 상숫값
μ_B, σ_B^2	Batch Mean & Variance	학습 안정성을 위해 현재 미니 배치(Mini-batch) 내에서 계산된 특징값들의 평균과 분산
γ, β	Scale & Shift Parameters	정규화된 값에 형태의 다양성을 복원해주기 위해 역전파로 학습되는 스케일(γ) 및 이동(β) 변수
ϵ	Epsilon	분모가 0이 되는 것을 방지하기 위해 분산에 더해주는 아주 작은 극소값(안정화 상수)

Proposed Framework

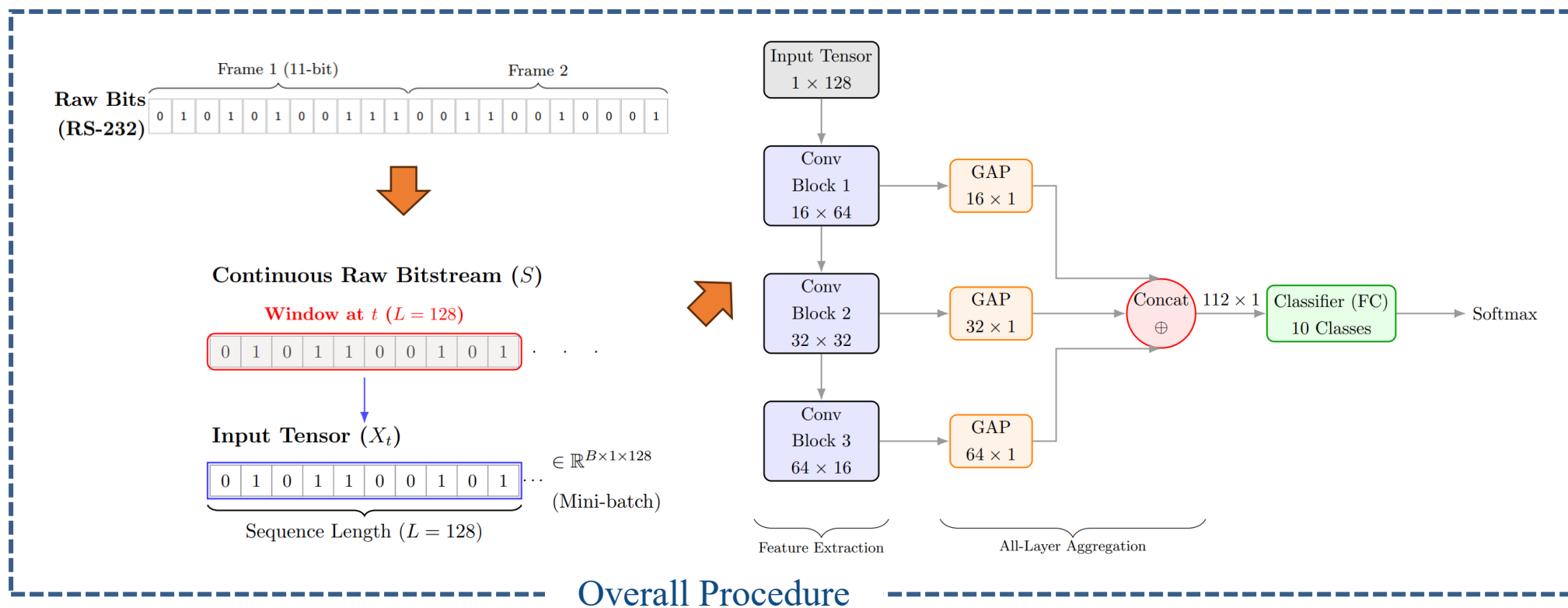
Notation and Definition

Symbol	Name of Symbol	Explain
L_l	Sequence Length	l 번째 계층에서 출력된 특징 맵의 시간축 길이 (예: Block 1은 64, Block 2는 32, Block 3은 16)
$\mathbf{F}_{c,t}^{(l)}$	Feature Value at Time t	시간 흐름(Sequence) 상의 특정 시점에 존재하는 개별적인 특징(Feature)의 스칼라 값
$\sum_{t=1}^{L_l}$	Summation over Time	시간 축의 첫 번째 지점부터 끝 지점까지의 모든 특징값들을 하나로 합산하는 연산
$\oplus$	Concatenation Operator	각 블록에서 압축된 서로 다른 1차원 벡터들을 차례대로 이어 붙여(Concat) 하나의 긴 벡터로 결합하는 연산자
$g^{(1)}, g^{(2)}, g^{(3)}$	Block-wise GAP Vectors	각각 미시적(Block 1), 중간적(Block 2), 거시적(Block 3) 패턴을 압축하여 담고 있는 블록별 요약 벡터
C_1, C_2, C_3	Channel Sizes	각 계층의 출력 채널 수. 병합된 최종 벡터의 길이는 이들의 합($16+32+64 = 112$ 차원)이 됨
$\mathbf{W}_{fc}, \mathbf{b}_{fc}$	FC Weight & Bias	최종 벡터($\mathbf{v}_{agg}$)를 10종의 장비 클래스로 사상(Mapping)하기 위한 분류기의 학습 파라미터
N_{class}	Number of Classes	분류하고자 하는 목표 장비의 총 개수 (본 연구에서는 식각, 증착 등 10개의 가상 장비, $N_{class} = 10$)
$\exp(z_k)$	Exponential Function	원시 점수(Logit) 간의 차이를 극대화하고, 이를 0보다 큰 양수로 변환하기 위한 자연 상수 지수 함수
B	Mini-batch Size	모델이 한 번에 병렬로 처리하고 학습하는 데이터(비트스트림 윈도우)의 묶음 크기
$y_{b,k}$	Ground Truth Label	실제 정답 라벨 (원-핫 인코딩 형식으로, 정답인 장비 클래스 위치에는 1, 나머지는 0의 값을 가짐)
θ	Model Parameters	오차(Loss)를 줄이기 위해 Adam Optimizer에 의해 지속적으로 업데이트되는 모델의 전체 가중치 집합

Proposed Framework

Overview

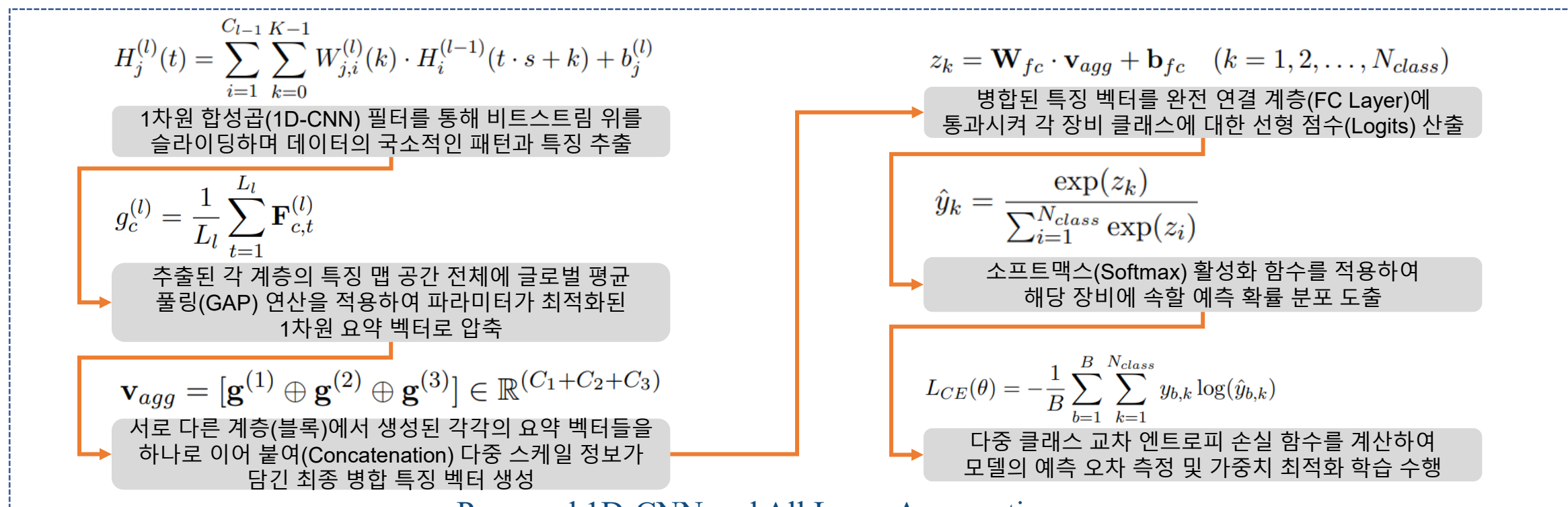
- 시리얼 통신을 통해 수신되는 비트스트림을 128Bit마다 Sliding Window 모델로 전달하고, 빠르고 가벼운 1차원 합성곱 신경망 필터를 통해 지역적 특징을 추출함.
- 모든 CNN Block에서 추출된 특징 맵을 압축 및 병합하여 종합 특징 벡터를 도출하고, 이를 통해 어느 정비에서 발송된 내용 인지를 식별함.



Proposed Framework

Neural Network for Protocol Classification

- Sliding Window 방식으로 병렬 연산이 가능한 1차원 합성곱 신경망을 통해 실시간으로 특징을 추출하며, 1계층에서는 미시적 특징(Start, Parity, End Bit 등)을 3계층에서는 거시적 특징(SECS-II 메시지 흐름이나 SML Tag 등)을 추출하게 됨.
- 반도체 통신의 식별에는 미시적/거시적 특징이 모두 중요하므로, 모든 계층의 결과물을 버리지 않고 모아서 사용하는 전 계층 집계(All Layer Aggregation) 메커니즘을 적용하여 장비를 식별함.



Proposed 1D-CNN and All Layer Aggregation

Experimental Settings

Dataset

- 본 연구를 위해 반도체 장비 10종에 대한 메시지 생성기를 제작하였으며, 이를 토대로 총 50,000개 규모의 시리얼 비트스트림 데이터 셋을 구축하였음.
- 각 장비에 대해서 SECS 기반의 다양한 시나리오들(대기, 가동, 알람, 레시피 전송 등)을 가정하여 메시지를 생성하도록 하였으며, 최대한 여러 종류의 메세지들을 골고루 발생시킬 수 있도록 제작하였음.

클래스 라벨	장비 종류 (Equipment Type)	데이터 수	비율
Class 0	노광 장비 (Photolithography Stepper)	5,000 개	10%
Class 1	식각 장비 (Dry Etcher)	5,000 개	10%
Class 2	화학기상증착 장비 (CVD, Chemical Vapor Deposition)	5,000 개	10%
Class 3	물리기상증착 장비 (PVD, Physical Vapor Deposition)	5,000 개	10%
Class 4	이온 주입 장비 (Ion Implanter)	5,000 개	10%
Class 5	화학적 기계 연마 장비 (CMP, Chemical Mechanical Polishing)	5,000 개	10%
Class 6	세정 장비 (Wet Cleaning Station)	5,000 개	10%
Class 7	감광액 제거 장비 (PR Asher / Stripper)	5,000 개	10%
Class 8	트랙 장비 (Track / Coater & Developer)	5,000 개	10%
Class 9	계측 및 검사 장비 (Metrology & Inspection)	5,000 개	10%
합 계	총 10종 반도체 단위 공정 설비	50,000 개	100%

Experimental Settings

Hyperparameter Settings

구분	Hyperparameter	설정값 (Value)	설명 및 비고 (Description)
네트워크구조	Input Sequence Length (L)	128	원시 비트스트림 슬라이딩 윈도우 크기
	Conv Block 1 Kernel Size (K1)	7	미시적 특징 추출용 1D 필터 크기 (출력 채널: 64)
	Conv Block 2 Kernel Size (K2)	5	중간 수준 패턴 추출용 1D 필터 크기 (출력 채널: 128)
	Conv Block 3 Kernel Size (K3)	5	거시적 메시지 구조 추출용 1D 필터 크기 (출력 채널: 256)
	Stride (s)	1	모든 합성곱 계층의 필터 이동 보폭
	Activation Function	ReLU	합성곱 계층의 비선형 활성화 함수
학습설정	Optimizer	Adam	경사 하강법 기반 가중치 최적화 알고리즘
	Learning Rate (α)	0.001	모델의 초기 학습률 (Learning Rate)
	Loss Function	Cross-Entropy Loss	10종 장비 다중 클래스 분류용 손실 함수
	Batch Size (B)	128	한 번에 학습할 미니 배치 크기
	Epochs	15	전체 50,000개 데이터셋의 학습 반복 횟수
	Dropout Rate	0.1	과적합(Overfitting) 방지를 위한 무작위 노드 비활성화 비율

Experimental Settings

Evaluation Measures

- 10종의 반도체 설비 통신 데이터를 얼마나 정확하고 안정적으로 식별하는지 객관적으로 검증하기 위해 데이터를 8:2 비율로 분할하여 5-겹 교차 검증(5-Fold CV)을 수행하여 평가하였음.
- 컴퓨팅 자원이 제한된 산업용 엣지(Edge) 환경에서의 실시간 구동 가능 여부를 입증하기 위해, 단일 샘플의 추론 지연 시간(Inference Latency)과 모델 파라미터 수를 측정하여 연산 효율성을 집중적으로 평가하였음.

Predict / Actual	Actual Position (P)	Actual Negative (N)
Predict Positive (P)	TP True Position (정답)	FN False Negative (오답)
Predict Negative (N)	FN False Negative (오답)	TP True Position (정답)

Confusion Matrix

정확도 (Accuracy) $\frac{TP + TN}{TP + TN + FP + FN}$	정밀도 (Precision) $\frac{TP}{TP + FP}$
재현율 (Recall) $\frac{TP}{TP + FN}$	조화 평균 (F1-Score) $2 \times \frac{Precision \times Recall}{Precision + Recall}$

핵심 분류 지표

Experimental Results

Comparison to Conventional Methods

- 제안하는 전 계층 집계 기반 1D-CNN 모델은 다중 클래스 프로토콜 분류 실험에서 **99.88%의 정확도와 0.998의 F1-Score를 달성**하며 기존 비교 알고리즘들의 식별 성능을 크게 상회하였음.
- 또한, 모델 파라미터 수를 0.2M 수준으로 대폭 경량화 하여 **추론 지연 시간을 41.6ms로 단축**시킴으로써, 자원이 제한된 마스터 엣지 환경에서도 통신 지연 없는 실시간 비트스트림 분석이 가능함을 입증하였음.

Model	Acc (%)	Prec	Recall	F1 Score	Params (M)	Latency (ms)
Proposed	99.88	0.998	0.998	0.998	0.2M	41.6
MLP	87.42	0.881	0.987	0.865	5.2M	85.2
LSTM	94.15	0.942	0.941	0.941	1.8M	142.7
Std 1D-CNN	96.80	0.970	0.968	0.967	0.9M	72.4

Experimental Results

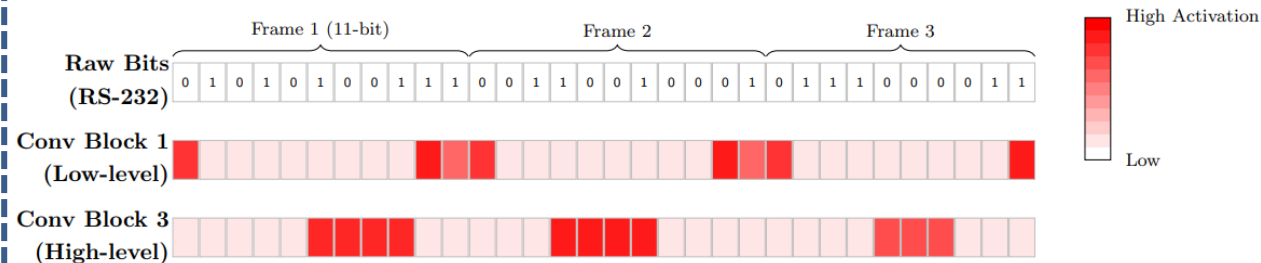
In-depth Analysis

- 본 연구는 1D-Grad-CAM 기반의 정성적 분석을 통해 인공지능이 실제 직렬 통신 규격의 핵심 제어 패턴을 정확히 추적하여 분류하고 있음을 보여줌으로써, 딥러닝 모델의 산업 현장 적용에 필수적인 해석 가능성과 신뢰성을 입증하였음.
- 또한 극도로 제한된 엣지 미들웨어 환경에서도 실시간 장비 식별이 가능함을 확인시킴으로써, 물리적 헤더가 부재한 레거시 반도체 설비의 완전 자동화 및 SDF 생태계 조성을 위한 실무적 기반 기술을 제시함.

$$L_{1D-Grad-CAM}^c = ReLU \left(\sum_k \alpha_k^c A_k \right) \quad \text{where } \alpha_k^c = \frac{1}{Z} \sum_t \frac{\partial y^c}{\partial A_k(t)}$$

- c : 대상 클래스
- k : 특징 맵 인덱스
- t : 시간 축 인덱스
- y^c : 클래스 c 에 대한 원시 예측 점수
- A_k : k 번째 활성화 맵
- $A_k(t)$: 활성화 값
- $\frac{\partial y^c}{\partial A_k(t)}$: 역전파 연산을 통해 구해진 기울기
- Z : 특징 맵의 전체 길이
- α_k^c : 특징 맵 중요도 가중치
- $\sum_k$: 가중합
- $ReLU$: 활성화 함수
- $L_{1D-Grad-CAM}^c$: 최종 1D-Grad-CAM 히트맵

1D-Grad-CAM 활성화 수식



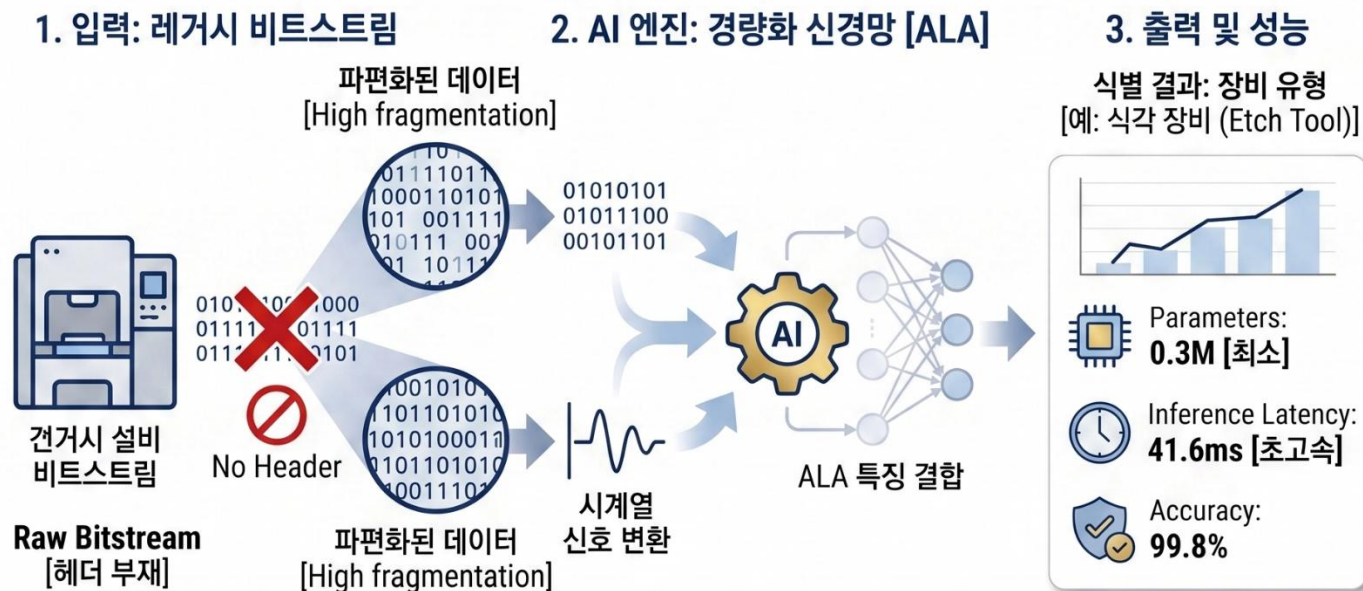
1. Conv Block1에서는 11bit로 나뉘어 있는 Frame의 시작과 끝 부분에 활성화 되어 있습니다.
이는 RS-232 직렬 통신의 Framing 규칙인 Start bit, Parity bit, End bit들의 위치를 정확하게 인식하고 있음을 의미합니다.
2. Conv Block3에서는 중앙의 데이터 bit 구간을 가로지르며 더 넓고 연속적인 형태로 활성화되어 있습니다.
네트워크의 깊이가 깊어짐에 따라 모델의 수용 영역이 넓어졌고, 여러 바이트가 조합되어 만들어내는 SECS-II 프로토콜의 논리적 메시지 내용을 식별하고 있음을 의미합니다.

1D Grad-CAM을 이용한 시리얼 비트스트림 계층별
활성화(Activation) 히트맵 시각화 결과

Conclusion

Conclusion

- 본 연구는 물리적 통신 헤더가 부재한 레거시 반도체 설비들을 엿지 환경에서 실시간으로 자동 식별하기 위해 프로토콜 비트스트림을 시계열 신호로 간주하고 경량화된 신경망으로 분류하는 프레임워크를 제안하였음.
- 기존 거대 AI 모델들이 마스터 미들웨어에서 유발하는 극심한 연산 부하 및 추론 지연 문제를 해결하고자, 제안 모델은 비트스트림의 특징을 병렬로 추출한 뒤 전 계층 집계(All-Layer Aggregation) 기술을 적용하여 파라미터 팽창 없이 다중 스케일 정보를 결합하였음.
- 기존 비교 알고리즘들과의 성능 평가에서 제안 알고리즘은 0.3M 수준의 적은 파라미터로 99.88%의 높은 정확도와 41.6ms의 낮은 지연 시간을 달성하였으며, 프리드먼 및 네메니 통계 검정을 통해 이러한 식별 성능 우위가 통계적으로 유의미함을 확인할 수 있었음.



Thank you

Reference

- [1] Zhong, R. Y., Xu, X., Klotz, E., and Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: a review. *Engineering*, 3(5):616–630.
- [2] Kim, J., Lee, J., Park, S. J., Lee, J., Song, B., and Moon, S. K. (2025). Software-defined factory: Paradigm shift in manufacturing towards industry 5.0. *International Journal of Precision Engineering and Manufacturing-Smart Technology*, 3(2):201–209.
- [3] Ahn, J., Yun, S., Kwon, J.-W., and Kim, W.-T. (2024). Literacy deep reinforcement learning-based federated digital twin scheduling for the software-defined factory. *Electronics*, 13(22):4452.
- [4] Koyasako, Y., Suzuki, T., Hatano, T., Shimada, T., and Yoshida, T. (2024). Demonstration of industrial ethernet protocol softwarization and advanced motion control for full software-defined factory network. *IEEE Access*, 12:104020–104030.
- [5] Iwao, T. (2018). Architecture of semiconductor equipment networks. *IEEE Transactions on Semiconductor Manufacturing*, 31(2):241–247
- [6] Moyne, J. and Iskandar, J. (2017). Big data analytics for smart manufacturing. *Processes*, 5(3):39.
- [7] Wang, Y. et al. (2024). Deep learning for unknown protocol reverse engineering: Challenges and opportunities. *IEEE Network*.
- [8] Bossert, G., Guilh'ery, F., and Hiet, G. (2014). Netzob: Inference of reverse-engineered communication protocols. *IEEE Security and Privacy*.
- [9] Ghimire, A. et al. (2025). A survey on application of ai on reverse engineering for software analysis and security. *IEEE Access*
- [10] Wei, X., Dai, H., Wang, Y., Shi, T., Sun, B., and Sun, J. (2026). A deep learning framework for industrial control protocol reverse engineering with multi-view attention and contrastive feature enhancement. *Engineering Letters*, 34(3):993–1000.
- [11] Chen, L. et al. (2025). Transre: Transfer learning based protocol reverse engineering using self-attention. *Journal of Network and Computer Applications*
- [12] Meng, X. et al. (2024). Protocolgpt: Prompting large language models for network protocol understanding. In *Proceedings of the 33rd USENIX Security Symposium*.
- [13] Fawaz, H. I., Forestier, G., Weber, J., Idoumghar, L., and Muller, P.-A. (2019). Deep learning for time series classification: a review. *Data mining and knowledge discovery*, 33(4):917–963.
- [14] Park, J., Kim, D.-W., and Lee, J. (2024). Calanet: Cheap all-layer aggregation for human activity recognition. In *Advances in Neural Information Processing Systems (NeurIPS)*.