

A Comparison of Meta-learning and Transfer-learning for Few-shot Jamming Signal Classification

Mi-Hyun Jin[†], Ddeo-Ol-Ra Koo, Kang-Suk Kim

GNSS R&D Center, Danam Systems, Anyang 13930, Korea

ABSTRACT

Typical anti-jamming technologies based on array antennas, Space Time Adaptive Process (STAP) & Space Frequency Adaptive Process (SFAP), are very effective algorithms to perform nulling and beamforming. However, it does not perform equally well for all types of jamming signals. If the anti-jamming algorithm is not optimized for each signal type, anti-jamming performance deteriorates and the operation stability of the system become worse by unnecessary computation. Therefore, jamming classification technique is required to obtain optimal anti-jamming performance. Machine learning, which has recently been in the spotlight, can be considered to classify jamming signal. In general, performing supervised learning for classification requires a huge amount of data and new learning for unfamiliar signal. In the case of jamming signal classification, it is difficult to obtain large amount of data because outdoor jamming signal reception environment is difficult to configure and the signal type of attacker is unknown. Therefore, this paper proposes few-shot jamming signal classification technique using meta-learning and transfer-learning to train the model using a small amount of data. A training dataset is constructed by anti-jamming algorithm input data within the GNSS receiver when jamming signals are applied. For meta-learning, Model-Agnostic Meta-Learning (MAML) algorithm with a general Convolution Neural Networks (CNN) model is used, and the same CNN model is used for transfer-learning. They are trained through episodic training using training datasets on developed our Python-based simulator. The results show both algorithms can be trained with less data and immediately respond to new signal types. Also, the performances of two algorithms are compared to determine which algorithm is more suitable for classifying jamming signals.

Keywords: jamming, meta-learning, transfer learning, classification

1. INTRODUCTION

전자전의 핵심 공격 수단 중 하나인 재밍은 전자파를 이용하여 무선 통신 체계를 방해, 마비, 무력화하는 행위이다. 고의적인 재밍 공격은 특정 주파수나 신호를 사용하지 못하도록 초고주파 신호를 목표 시스템에 방사하는 형태로 이뤄진다. 또한 물리적이

Global Navigation Satellite System (GNSS)와 같이 수신 신호 전력이 낮은 통신 시스템일수록 효과적이다. GNSS는 사용자에게 위치, 경로 및 시각 정보를 제공하는 위성 시스템으로서, 국가 인프라의 필수 요소가 되었을 뿐만 아니라 지휘통제 체계나 유도무기 체계에서도 핵심 기술로써 활용되고 있다. 그러나 위성 신호의 크기가 잡음보다 낮아 공격에 취약한 단점을 가지고 있으므로 전자전에서 위협을 가장 많이 받는 요소 중 하나이다. 따라서 이에 대응하기 위한 재밍 대응 기술 연구가 국내외에서 광범위하게 이루어지고 있다.

재밍 대응 기술은 크게 물리적 대응을 위한 재머 위치 추적 기술과 전자 보호를 위한 항재밍 기술로 구분할 수 있다. 대표적인 재머 위치추적 기법으로는 Time Difference of Arrival (TDOA) 측정치 기반 위치결정 기법 (Smith & Abel 1987), Angle of Arrival (AOA) 측정치 기반 위치결정 기법 (Schmidt 1986)을 들 수 있으며, 대표적인 항재밍 기술로는 배열 안테나인 Controlled

Received Jul 25, 2022 Revised Aug 01, 2022 Accepted Aug 04, 2022

[†]Corresponding Author

E-mail: mhjin@danam.co.kr

Tel: +82-31-538-6020 Fax: +82-31-425-4308

Mi-Hyun Jin <https://orcid.org/0000-0002-4985-9946>

Ddeo-Ol-Ra Koo <https://orcid.org/0000-0002-9816-5844>

Kang-Suk Kim <https://orcid.org/0000-0003-4177-6545>

Reception Pattern Antenna (CRPA)를 기반으로 한 Space Time Adaptive Process (STAP) 기법 (Ward 1994)과 Space Frequency Adaptive Process (SFAP) 기법 (Moore 2002)이 있다. 각 기법은 고유의 장단점을 가지고 있으며 재밍의 유형에 따라 적용 가능한 기법과 성능이 크게 변화한다. 특히 디지털 신호 처리에 기반한 STAP 및 SFAP 등은 매우 효과적인 알고리즘이지만, 모든 유형의 재밍 신호에 대해 동일하게 우수한 성능을 내지 못한다. 만약 적절하지 않거나 과도한 대응 기술을 적용할 경우 항재밍 기법의 성능 열화가 발생하며 알고리즘의 연산량이 필요 이상으로 증가할 수 있다. 이때 재밍 신호를 미리 식별하여 항재밍 알고리즘을 최적화한다면 높은 대응 성능을 얻을 수 있을 뿐만 아니라 불필요한 연산량을 줄임으로써 수신기 시스템의 동작 안정성을 확보할 수 있다.

재밍 신호 식별에 대해서는 Power Spectral Density (PSD) 분석을 기반으로 한 식별 기법들이 제안된 바 있다 (Fadaei 2016, Bazec & Dimc 2018). 이러한 기법들은 시각적인 차이가 명확하여 분류가 용이해 보이지만, 자동 식별을 위한 특성의 추출이 어려운 단점을 갖는다. 또한 다중 경로 추정기를 이용한 식별 기법 (Gross & Humphreys 2017)도 제안되었으며, 기만 신호를 포함하여 식별이 가능하지만 상관기 이후의 값을 사용하기 때문에 상관기의 성능에 영향을 받으며 신호의 전처리가 불가능하다는 한계를 보인다. 마찬가지로 국내에서는 재밍 식별을 위해 Spectral Correlation Function (SCF) 및 wavelet coherence를 이용한 매칭 기반 기법이 제안된 바 있다 (Jin et al. 2018). 그러나 SCF 및 wavelet coherence를 이용한 식별 방안들은 높은 연산량과 긴 식별 소요 시간이라는 단점이 존재한다. 또한 템플릿에 의해 성능이 결정될 뿐만 아니라 템플릿이 사전에 존재해야 하므로 새로운 종류의 재밍 신호에 대해서 즉각적인 대응이 어려운 단점 또한 갖는다. 한편 최근 인공지능이 각광받으며 Support Vector Machines (SVM)과 Convolution Neural Networks (CNN)을 사용하는 재밍 식별 기법이 국내 및 국외에서 다수 제안되고 있다 (Ferre et al. 2019, Lee et al. 2019, Yoo 2020). 제안된 기법에서는 학습 수행 시 매우 많은 데이터가 필요하며 새로운 분류가 추가될 경우 새로운 학습을 거쳐야 한다. 그러나 재밍 공격은 자주 발생하지 않으며, 시뮬레이션을 이용하여 생성한 데이터는 실 수신 데이터와 크게 달라 활용할 수 없어 학습 데이터를 확보하기 어렵다. 또한 앞서 제안된 다른 기법과 마찬가지로 새로운 신호에 대한 식별이 불가능한 단점이 존재한다.

본 논문에서는 인공지능에 기반하면서도 위와 같은 기법들의 단점을 보완할 수 있고 새로운 신호에 대한 빠른 판단이 가능할 수 있도록, 전이 학습 (transfer learning) 및 메타 러닝 (meta-learning) 기반 재밍 신호 식별 알고리즘을 제안한다 (Pan & Yang 2010, Finn et al. 2017, Jin et al. 2021). 두 기법은 퓨샷 러닝 (few-shot learning; FSL)을 위한 학습 방식으로, 적은 양이면서 새로운 데이터 셋을 효율적으로 학습하기 위하여 제안되었다. 전이 학습은 적절하게 훈련된 사전 모델이 존재할 경우 새로운 신호 유형에 대해 기존 망을 일부 튜닝하여 식별이 가능하다. 또한 메타 러닝은 학습에 필요한 변수를 자동으로 최적화함으로써, 새로운 신호에 대해 빠른 튜닝이 이뤄져 적은 양의 데이터로도 즉각적으로 식별이 가능하다. 재밍 신호 식별을 위해

Model-Agnostic Meta-Learning (MAML)을 사용한 기존 연구에서 MAML을 이용하여 식별이 가능함이 증명된 바 있으나 (Jin et al. 2021), 두 방식 중 어떤 방식이 재밍 신호 식별에 대해 보다 효율적인지는 확인된 바 없다. 따라서 기존 논문을 발전시킨 본 논문에서는 두 알고리즘을 적용한 재밍 신호 식별 성능을 도출한 후 성능 비교도 함께 수행한다. 모델 학습을 위한 데이터는 항재밍 알고리즘 입력 데이터인 공분산 데이터를 사용하였으며, 훈련 및 테스트 데이터 셋 구성을 위해 재밍 신호 수신 시 GNSS 수신기 내에 구현된 항재밍 알고리즘의 입력 데이터를 수집하였다. 메타 러닝 모델로는 MAML을 사용하였으며, 전이 학습의 사전 학습 모델로는 CNN을 사용하였다 (Jin et al. 2021). 두 모델은 개발한 파이썬 기반 시뮬레이터에서 훈련 태스크를 이용한 에피소드 훈련을 통해 재밍 신호의 유형을 학습한다. 최종적으로 시험 태스크를 이용하여 식별 성능을 획득하고 두 기법의 성능을 비교함으로써 제안한 방안을 검증하고 결론을 도출한다.

2. FEW-SHOT LEARNING APPROACH FOR JAMMING CLASSIFICATION

현재의 AI 기술은 최적의 성능을 도출하기 위하여 많은 양의 데이터를 필요로 한다. 또한 매우 적은 예제를 이용하여 학습을 수행할 경우 보편적인 결과를 내지 못한다. 그에 비해 사람은 적은 수의 예제를 보고서도 쉽게 응용력을 발휘할 수 있으므로, AI와 사람의 격차를 좁히는 방향으로 기술을 발전시키는 패러다임이 AI 개발 동향의 한 축을 차지하였다. 그 중 하나가 제한된 수의 데이터로 지도 학습 및 강화 학습을 수행하는 문제인 FSL이다 (Wang et al. 2021). 기본적으로는 안전이나 사생활 보호 등의 문제로 인해 불가능에 가까운 정도로 어려운 상황에서 획득한 소수의 데이터가 존재함을 가정하며, 더 나아가 행동 모방이나 언어 생성 등의 문제를 다룰 수 있다. 또한 이미지 식별 및 추출, 행동 인지, 문장 번역 등 다량의 데이터가 필요한 문제도 보다 적은 예제를 가지고도 학습이 가능함을 목표로 한다. FSL 문제를 해결한다면 데이터 수집에 대한 부담이 감소함으로써 시간 및 비용을 절감할 수 있으므로 현재 관련 연구가 활발하게 진행되고 있다. 그 중 각광받는 접근 방식으로는 전이 학습 (Pan & Yang 2010), 메타 러닝 (Finn et al. 2017), 비대칭 학습 (He & Garcia 2009), 액티브 러닝 (Settles 2009) 등이 있다. 안타깝게도 모든 경우에 있어 최고의 성능을 제공하는 접근 방식은 현재 존재하지 않으며, 문제의 유형 및 데이터의 양, 그리고 신경망의 구조에 따라 각기 다른 성능을 보인다.

재밍 신호 식별은 수집할 수 있는 데이터의 수가 적고, 재밍 신호를 수신한 수신기 외의 다른 경로를 통하여 데이터를 생성하기도 어렵기 때문에 전형적인 FSL 문제에 해당한다. 재밍 신호를 위한 지도 학습 수행 시 데이터 셋의 구성 데이터 수는 수백개를 넘기기 어려우며, 신호 송신 목적이 공격인 이상 학습시킨 신호 유형 외의 새로운 신호 유형이 수신될 가능성도 높다. 이러한 상황에 대응하기 위하여 본 논문에서는 전이 학습 및 메타 러닝을 재밍 신호 식별을 위한 접근 방식으로 고려하였으며, 이에 기반한 세부 내용은 하위 절에 기술하였다.

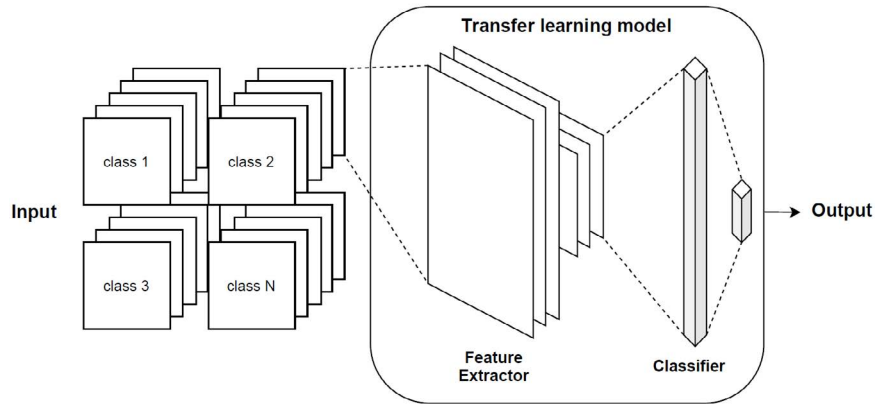


Fig. 1. The structure of basic transfer learning model.

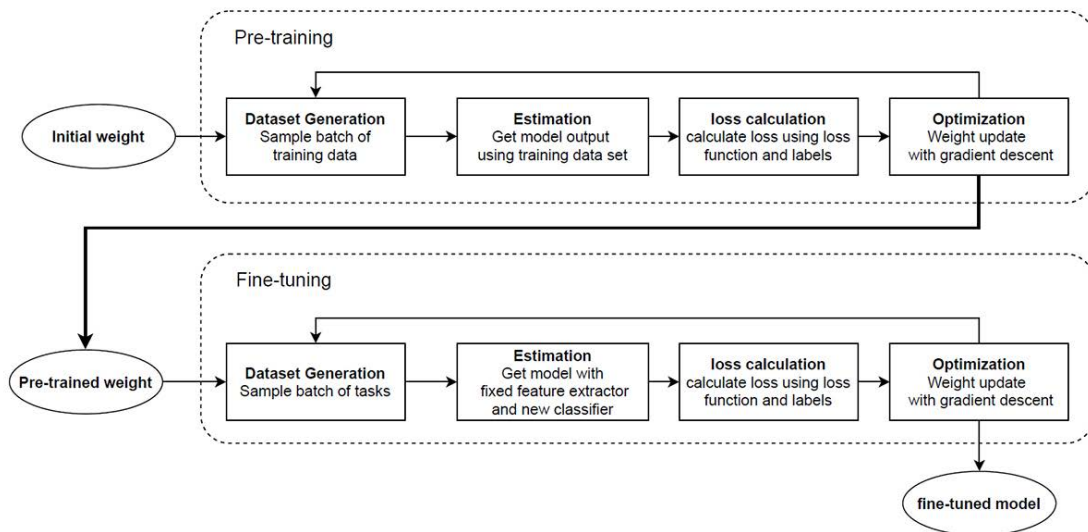


Fig. 2. Block diagram of implemented transfer learning model.

2.1 Transfer Learning

전이 학습은 충분한 데이터를 이용하여 학습된 모델의 지식, 학습 데이터의 양이 부족하지만 형태가 유사한 모델로 전달함으로써 FSL 문제를 해결하고자 하는 학습 방식이다. 답러닝은 방대한 데이터가 필요하며, 그 데이터에 대한 라벨링이 전부 완료되어야 하고, 신경망의 크기가 비대하여 필요한 연산량이 높은 한계점을 가진다. 또한 학습되지 않은 범주인 새로운 데이터를 분류하고자 하는 퓨샷 태스크 (few-shot task) 문제의 해결이 불가능한 문제가 있다. 전이 학습은 이러한 답러닝의 한계를 극복하기 위하여 제안되었다.

기존에 보유했던 많은 양의 데이터로 적절하게 훈련된 사전 모델이 존재할 경우, 그 모델을 기반으로 적은 양의 새로운 데이터에 대한 최적화를 수행함으로써 새로운 문제에 대응할 수 있다. 이때 최적화는 사전 학습된 모델의 가중치의 일부를 새로운 데이터를 이용하여 다시 학습시키는 과정을 의미하며, 일반적으로 모델의 종단에 위치한 선형 레이어의 가중치를 이용한다. 전

이 학습을 적용하기 위해서는 사전 학습 모델에 사용한 데이터가 목표하는 문제 해결에 사용될 데이터와 같은 유형 (도메인)이어야 하며, 사전에 훈련된 모델이 존재해야 할 뿐만 아니라 모델의 성능에도 영향을 받는다는 한계점이 존재한다. 기본적인 전이 학습의 구조는 Fig. 1과 같다.

전이 학습의 신경망 모델은 크게 특징 추출기 (feature extractor)와 분류기 (classifier)로 구분할 수 있다. 사전 훈련을 진행함으로써 신경망 모델의 특징 추출기와 분류기는 동시에 학습되며 사전 훈련을 위한 데이터셋이 많으면 많을수록 특징 추출기의 성능은 향상된다. 이후 새로운 데이터에 대한 FSL을 진행할 때, 동일한 구조의 신경망이 보유한 특징 추출기에 사전 훈련된 특징 추출기가 보유하고 있는 지식인 가중치를 전이 (transfer) 시킨다. 이때 분류기는 데이터에 적합하도록 새롭게 정의된 선형 레이어이며, FSL을 위한 데이터를 학습시킴으로써 선형 레이어의 미세조정 (fine-tuning)을 수행한다. 본 논문에서 구현한 전이 학습 과정은 Fig. 2와 같다.

먼저 사전 학습 (pre-training) 모델에 임의의 가중치로 초기화

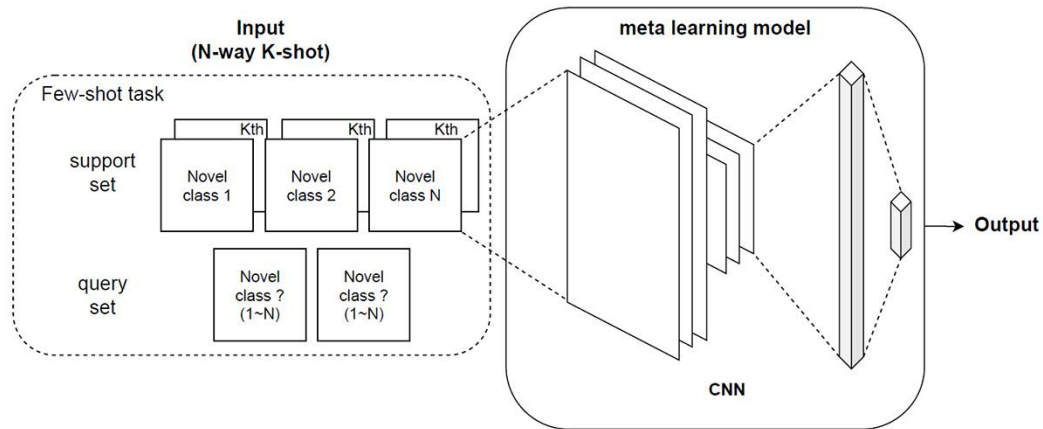


Fig. 3. The structure of basic meta learning model.

를 수행한 후 딥러닝을 위한 학습과 동일한 방식으로 대량의 라벨링된 데이터 셋을 이용하여 학습을 수행한다. 이때 사전 학습을 위한 데이터셋이 FSL 문제를 위한 데이터셋과 유사한 도메인을 가질수록 더 우수한 FSL 문제 해결 능력을 갖는다. 학습 성능이 수렴할 정도로 충분한 양의 데이터를 이용한 학습이 완료되었다면, 미세 조정 (fine-tuning) 모델의 특징 추출기 가중치를 사전 훈련 모델의 값으로 고정시키고 분류기의 가중치를 임의의 값으로 초기화한다. 이를 통해 미세 조정 모델의 특징 추출기는 거의 학습을 수행하지 않았음에도 불구하고 입력 데이터의 유의미한 특징을 추출할 수 있는 능력을 가지며, 분류기는 퓨샷 데이터를 이용한 적은 수의 학습으로도 데이터의 라벨을 식별할 수 있는 능력을 갖는다.

특징 추출기는 데이터의 유형에 따라 다양한 형태의 신경망 구조를 가질 수 있으며, 본 논문에서는 분류 문제에 적합한 Convolution Neural Network (CNN) 구조를 구현하였다. 이 구조는 특징 추출을 담당하는 합성곱층 (convolutional layer), 배치 정규화층 (batch-norm layer), 풀링층 (pooling layer) 레이어로 구성되어 있으며, 합성곱층과 배치 정규화층은 3번 중첩된 구조를 가지도록 설계하였다. CNN만 단독으로 사용할 경우 일반적으로 종단에 완전연결 계층 (fully-connected layer)가 존재하지만, 전이 학습에서는 분류기가 별도로 존재하므로 추가하지 않았다. 구현한 전이 학습 모델은 이어 설명할 메타 러닝 모델과 동일한 데이터셋을 이용하여 훈련되었다.

2.2 Meta-learning

메타 러닝은 FSL과 별도로 제안된 분야이지만, FSL 문제를 해결할 수 있는 머신러닝 기법 중 하나로 각광받고 있다. 메타 러닝은 학습 방법 자체를 학습하고자 하는 방식으로, 사람이 매우 적은 수의 예시를 보고도 효율적인 구별 방법을 찾아내듯이 소수의 데이터로도 분류가 가능한 학습 방법을 찾아내고 일반화하여 다른 문제에 적용한다. 이 방식은 사전 학습 모델을 충분히 훈련시키기 위해서는 반드시 유사한 문제에 대한 대량의 데이터가 필요하다는 전이 학습의 단점을 보완할 수 있다.

메타 러닝의 접근 방식은 크게 모델 기반 접근 방식, 거리 기

반 접근 방식 및 최적화 기반 접근 방식으로 나뉜다. 모델 기반 접근 방식은 고속 학습에 특화된 모델을 적용하는 방식으로, 외부 메모리를 이용하는 Memory-Augmented Neural Networks (MANN) 모델 (Santoro et al. 2016)이나, 가중치를 고속으로 업데이트하고자 하는 MetaNet (Munkhdalai & Yu 2017)을 이용한 방식들이 이에 해당한다. 거리 기반 접근 방식은 커널 함수에 따라 성능이 변화하며, Siamese Network (Koch 2015)와 Matching Networks (Vinyals et al. 2016) 등이 이에 해당한다. 이 방식은 커널 함수를 이용하여 데이터간 거리를 계산하기 때문에, 입력 데이터의 전처리 결과가 성능에 큰 영향을 미친다. 모델 기반 방식 및 거리 기반 방식은 구현이 복잡하며 모델과 커널 함수의 결정이 성능에 큰 영향을 미치기 때문에 유연성이 부족하다는 단점이 있다. 한편 최적화 기반 접근 방식은 모델의 최적화 알고리즘을 적은 수의 예제만을 활용하여 더 효율적으로 학습하는 알고리즘으로 변경하는 방식으로, Long Shot-Term Memory (LSTM)에 적용하기 위한 meta-learner (Ravi & Larochelle 2017)와 모든 모델에 범용적으로 적용 가능한 Model-Agnostic Meta-Learning (MAML) (Finn et al. 2017) 등이 있다. 그 중 MAML은 최근 각광받는 방식으로, 모델과 입력 데이터에 구애받지 않을 뿐만 아니라 구현 및 적용이 간단한 장점이 있다. 또한 특정 데이터에 대해 가중치를 최적화하지 않았음에도 불구하고 그에 준하는 성능을 확보할 수 있다. 본 논문에서는 메타 러닝 적용을 위해 여러 모델 중 기존 연구 (Jin et al. 2021)에서 구현하였던 MAML 및 그에 기반한 MAML+ 알고리즘을 구현하였으며 구조 및 과정은 Figs. 3, 4와 같다.

먼저 다수의 태스크로 구성된 샘플 배치를 생성하고, 하나의 태스크 데이터를 이용하여 지역 모델을 통과한 서포트 셋이 갖는 오차를 계산하고 최적화를 수행한다. 이후 지역 모델의 가중치를 갱신하고 동일 태스크에 대한 최적화를 더 이상 가중치의 변화가 발생하지 않을 때까지 반복하며 이를 내부 루프로 정의한다. 가중치가 수렴했다면 내부 루프를 종료하면서 쿼리 셋이 갖는 오차를 계산하여 외부 루프로 전달한다. MAML의 모델을 f_θ 로 간주하고 모델 가중치를 θ 로, 샘플 배치 안의 i 번째 태스크를 T_i 로 정의할 경우 내부 루프에서의 오차 및 가중치 갱신에 대한 식은 Eq. (1)과 같다 (Finn et al. 2017).

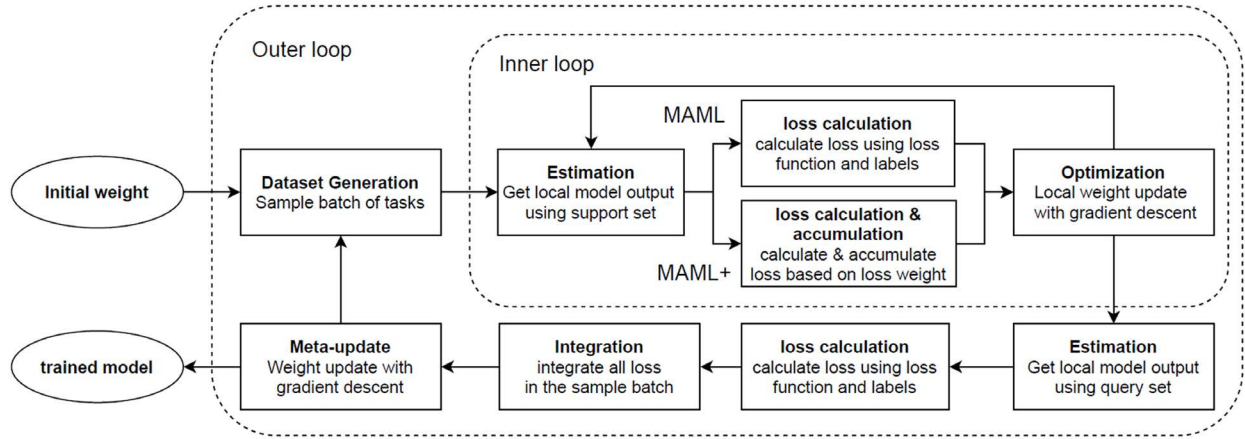


Fig. 4. Block diagram of implemented meta learning model (MAML).

$$\begin{aligned}\theta'_i &= \theta - \alpha \nabla_{\theta} \mathcal{L}_{T_i}(f_{\theta}), \text{iter} = 0 \\ \theta'_i &\leftarrow \theta'_i - \alpha \nabla_{\theta'_i} \mathcal{L}_{T_i}(f_{\theta'_i}), \text{iter} > 0\end{aligned}\quad (1)$$

여기에서 내부 루프의 가중치 스텝 크기 α 는 임의의 고정된 값을 갖는다. 내부 루프의 모델은 MAML의 모델과 완전히 동일하나, 가중치 θ'_i 가 갱신되더라도 그 값이 외부로 전달되지 않는 임시 가중치를 갖는 모델이다. 외부 루프로 전달된 쿼리 세트의 오차는 미니 배치에 포함된 모든 태스크가 내부 루프를 거칠 때까지 누적된다. 적분이 완료된 오차는 MAML의 모델 가중치를 갱신하기 위해 사용되며, 메타 업데이트라고 불리는 이 과정을 통해 가중치가 일반화될 수 있다. 하나의 샘플 배치를 이용한 훈련을 하나의 에피소드라고 정의할 수 있으며, 훈련을 위해서 다수의 에피소드를 반복한다. 한 에피소드 안에서 누적된 오차와 이에 따른 외부 루프에서의 가중치 갱신 식은 Eq. (2)와 같다 (Finn et al. 2017).

$$\theta \leftarrow \theta - \beta \nabla_{\theta} \sum_{T_i \sim p(T)} \mathcal{L}_{T_i}(f_{\theta'_i}) \quad (2)$$

여기서 β 는 메타 업데이트를 위한 학습률을 의미한다. MAML+의 경우 MAML과 대부분 동일하게 동작하지만 Eq. (1)의 스텝 크기 α 가 훈련 회수에 따라 값이 변화하며, 내부 루프에서의 오차가 지속적으로 누적된 후 외부 루프로 반환되는 차이점이 존재한다.

Fig. 3에서, MAML의 모델은 성능을 비교할 수 있도록 전이 학습의 미세 조정 모델과 동일한 구조의 CNN을 사용하였다 (Jin et al. 2021). 전이 학습에서 사전 훈련 모델의 학습을 위해 라벨이 정의된 대량의 데이터를 입력한 것과 달리, 메타 러닝 모델의 입력으로는 서포트 세트와 쿼리 세트로 구성되어 각 에피소드마다 새롭게 정의된 라벨을 갖는 FSL 태스크가 사용된다. 이 구조의 데이터셋은 전이 학습의 미세 조정 모델에도 동일하게 인가되었으며 3장에서 세부적으로 설명하였다.

3. DATASET

3.1 Data Features

본 논문의 재밍 신호의 식별 결과는 항재밍 알고리즘의 성능

을 향상시키기 위해 제공된다. 따라서 수신기에는 이미 항재밍 알고리즘이 존재하며, 구현 및 운영의 편의성을 고려할 경우 항재밍 알고리즘의 입력인 신호 공분산을 모델의 입력으로 사용하는 것이 별도의 데이터를 생성하는 것보다 유리하다. 공분산 확보 시 재밍 환경으로 최대 3개의 재밍 신호가 수신기에 입사하는 경우를 고려하였으며, 재밍 신호 유형으로는 정현파 신호인 Continuous Wave (CW) 신호와 각각 다른 중심주파수를 갖는 CW 신호를 중첩시킨 Multi-CW (MCW), 중심주파수가 변화하는 Frequency Modulation (FM) 신호, 마지막으로 광대역 신호인 Additive White Gaussian Noise (AWGN) 신호를 고려하였다. 최종적으로 수신되는 수신 신호는 1개의 단일 유형 신호, 3개의 단일 유형 신호, 그리고 경우에 따라 서로 다른 유형을 조합한 신호를 사용하였다. 이 중 AWGN 신호가 포함된 신호의 경우 훈련용 데이터셋에 포함시키지 않았으며, 오로지 시험을 위해서만 사용되었다.

항재밍 알고리즘으로 N개의 소자 배열 안테나를 사용하고 M개의 탭을 갖는 STAP 알고리즘을 고려할 경우 모델의 입력은 $N \times M$ 크기의 신호 공분산이 된다. 이때 공분산 배열의 절대적인 값은 재밍 신호의 세기와 하드웨어의 특성 및 신호 처리 결과에 따라 변화하므로 모델의 입력으로 바로 사용하기에는 적합하지 않다. 따라서 데이터 전처리를 위하여 최대-최소 정규화 및 Z-score 정규화를 수행하였으며 (Jin et al. 2021), 신호 유형별 데이터 전처리 결과의 일부를 Figs. 5와 6에 나타내었다.

3.2 Few-shot Learning Task

FSL는 딥러닝 등 기존의 학습 방식과 다른 방식으로 훈련을 진행하므로, 입력 데이터 또한 다른 구조를 갖는다. 샘플 배치 안에 포함된 하나의 FSL 데이터는 하나의 태스크 (task)로 불리며, 태스크 안에 포함된 클래스는 기존의 라벨을 갖는 것이 아니라 매 태스크마다 새롭게 정의된 새로운 라벨을 갖는다. 각 태스크를 구성하기 위해 다수의 클래스 중 k개의 클래스를 랜덤하게 선정한다면 포함된 클래스는 새롭게 정의된 1~k 사이의 라벨을 갖게 된다. 이때 하나의 클래스마다 n개의 샘플을 보유할 경우 이를

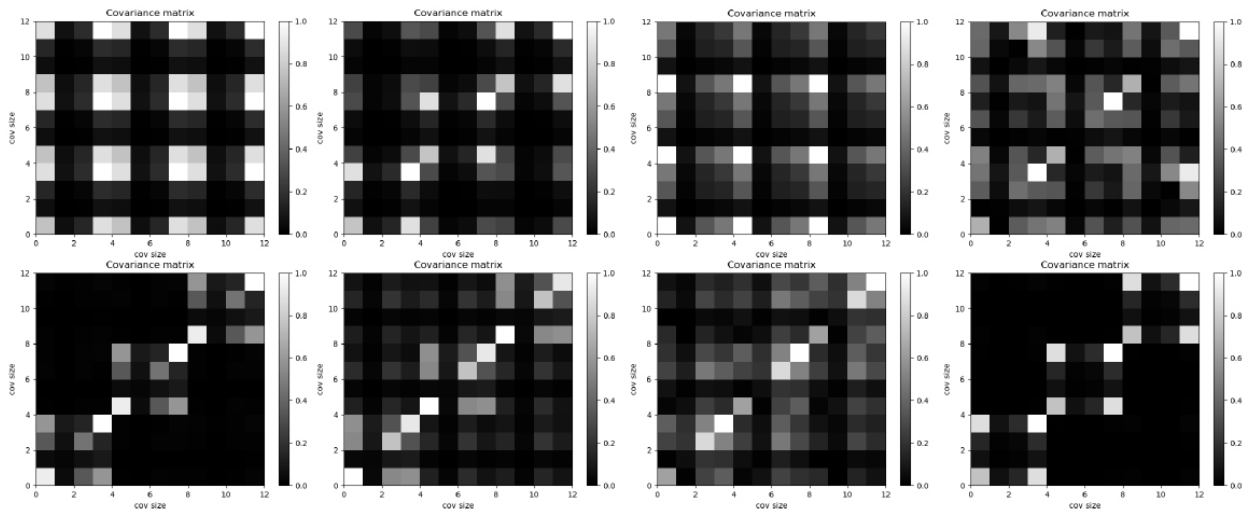


Fig. 5. Covariance matrix of jamming signal in meta-training dataset. Clockwise from top-left: 1CW, 1MCW, 3CW, 3MCW, 1FM, 1FM/2MCW, 2FM/1MCW, 3FM

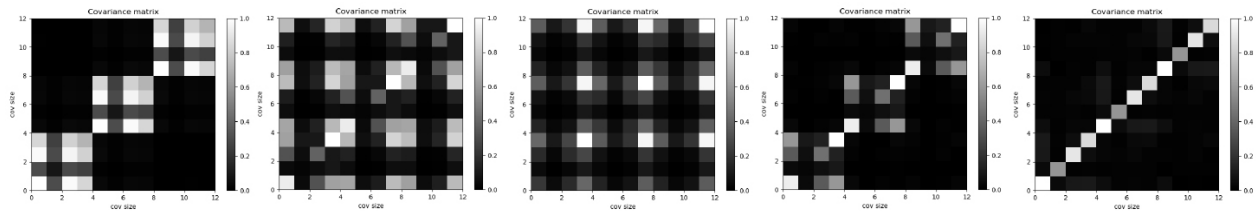


Fig. 6. Test configuration diagram for jamming signal data collection.

Table 1. Meta-training and meta-test dataset of MAML/MAML+ and transfer learning.

Dataset	FSL model	
	MAML/MAML+	Transfer learning
Meta-training	1CW, 1MCW, 3CW, 3MCW, 1FM, 1FM/2MCW, 2FM/1MCW, 3FM	The meta-training dataset of MAML/MAML+ is augmented with rotations by 90, 180, 270 degrees (Number of classes quadrupled)
Meta-test 1	1AWGN, 1CW/2AWGN, 2CW/1AWGN, 3AWGN, No jamming	
Meta-test 2	1CW, 1MCW, 3CW, 3MCW, 1FM, 1FM/2MCW, 2FM/1MCW, 3FM, 1AWGN, 1CW/2AWGN, 2CW/1AWGN, 3AWGN, No jamming	

k-way n-shot 태스크로 정의할 수 있다.

모델 훈련을 위한 데이터셋이 크게 학습 데이터셋과 테스트 데이터셋으로 나뉘듯이, FSL 데이터셋도 모델 학습 시에 사용하는 메타-학습 데이터셋과 모델 평가를 위한 메타-테스트 데이터셋으로 나뉜다. 두 데이터셋은 보편적으로 겹치지 않고 서로 다른 클래스를 가지며, 메타-학습 데이터셋에서 태스크 배치를 생성한 후 배치 내의 모든 태스크를 이용하여 학습을 수행하는 것을 하나의 에피소드 (episode)로 정의할 수 있다. 각 태스크는 내부적으로 서포트 셋 (support set)과 쿼리 셋 (query set)으로 나뉘며 훈련 혹은 테스트 여부에 따라 역할이 달라진다. 메타-훈련 데이터셋에서 생성한 태스크의 서포트 셋은 새로운 라벨을 갖는 데이터를 지역 모델이 학습하기 위한 데이터, 쿼리 셋은 서포트 셋을 이용한 훈련 결과에 따라 모델 전체에 대한 미세 조정을 수행하기 위한 데이터이다. 이때 쿼리 셋의 클래스는 서포트 셋에 존재하는 클래스 중 하나에서 임의로 선택되며, 쿼리 셋의 라벨 또한 서포트 셋에서 동일한 클래스가 갖는 라벨로 정의된다. 한

편 메타-테스트 데이터셋에서 생성한 태스크의 서포트 셋은 새로운 클래스에 대한 학습을 수행하기 위한 데이터, 쿼리 셋은 모델 성능을 평가하기 위한 데이터이다. 즉 메타-학습 데이터셋에서 생성한 다수의 태스크를 이용하여 에피소딕 (episodic) 학습을 완료한 후 메타-테스트 데이터에서 생성한 태스크들의 쿼리 셋에 대한 예측 성능이 FSL 모델 성능이 된다. 이때 FSL 문제에서 학습 성능을 지속적으로 확인하고 미세 조정을 수행하기 위해서는 학습 데이터셋과 다른 클래스를 갖는 검증 데이터셋을 이용하는 것이 일반적이나, 본 논문에서 생성 가능한 재밍 신호의 유형이 제한적이었기 때문에 별도의 검증 데이터셋을 두지 않았다.

본 논문에서는 재밍 신호의 식별을 목표로 하며, 모델의 성능을 정확히 확인하고자 할 경우 메타-테스트 데이터셋에는 새로운 유형의 신호만을 클래스로 정의하여야 한다. 그러나 항재밍 성능 개선 관점으로 볼 때 신규 신호에 대한 식별 성능 확인도 중요하지만 기존 신호에 대한 식별 성능 확인 역시 중요하다. 따라서 메타-테스트 데이터셋을 Table 1과 같이 2가지 유형으로 구성

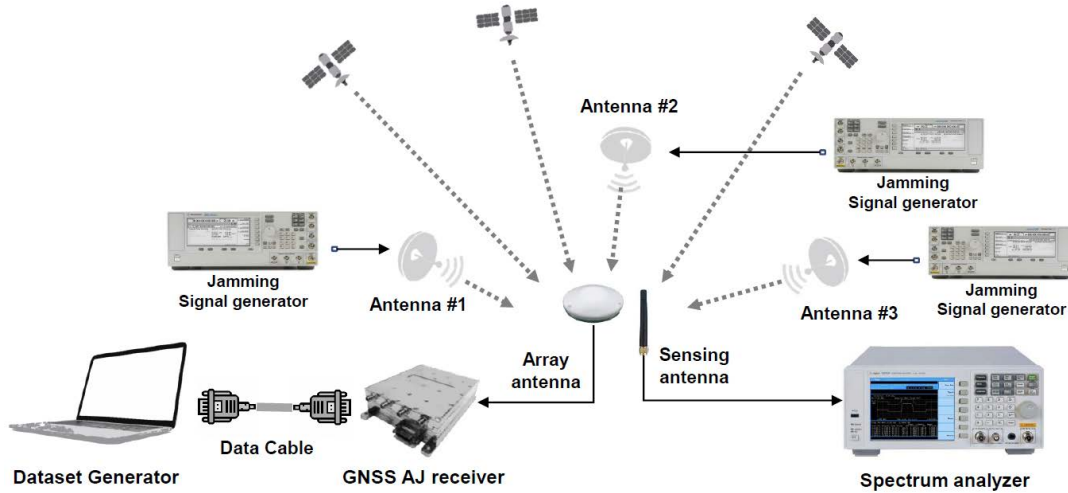


Fig. 7. Test configuration diagram for jamming signal data collection.

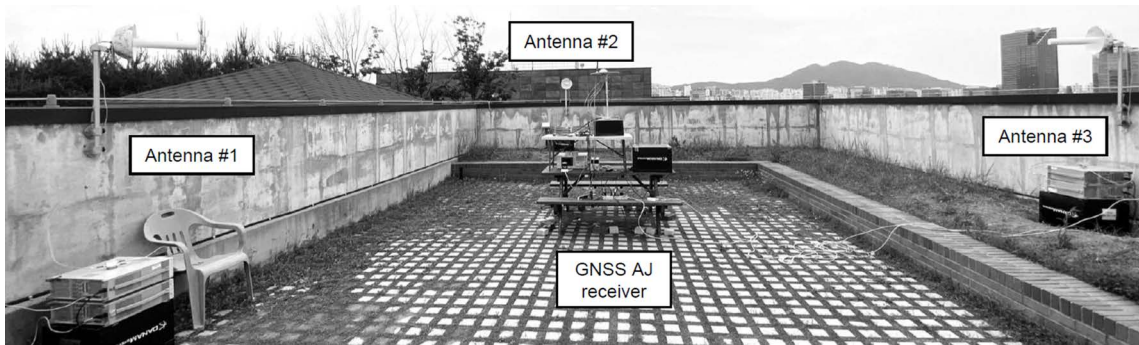


Fig. 8. Test environment for jamming signal data collection.

하였다.

첫 번째는 새로운 유형의 신호만을 이용하여 메타-테스트 데이터셋을 구성하였을 경우, 두 번째는 메타-학습 데이터셋의 클래스인 기존 유형의 신호와 새로운 유형의 신호를 전부 메타-테스트 데이터셋의 클래스로 구성하였을 경우이다. 다만 동일한 클래스라 하더라도 학습 데이터셋과 테스트 데이터셋의 샘플은 동일하지 않은 샘플로 구성되었다.

본 논문에서 학습을 위해 생성한 태스크는 5-way 1-shot의 구조를 가지며, 쿼리 셋은 서포트 셋에 존재하는 클래스 중 랜덤하게 선정된 3개의 클래스로 구성하였다. 훈련 성능을 높이고 과적합을 방지하기 위하여 데이터 샘플에 가우시안 블러, 축 회전 등의 변형을 적용하였다. 또한 전이 학습 모델의 경우 많은 양의 데이터를 훈련하여 학습을 시켜야 하는 특성상 메타-학습 데이터셋에 사이즈 변환, 데이터 추출 등의 전처리를 추가하여 상대적으로 샘플 수를 증가시켰으며, 각 신호 유형에 90도 배수 회전을 적용하여 데이터셋의 클래스를 증가시켰다. 반면 MAML 및 MAML+는 지나친 데이터 전처리 및 추가적인 클래스가 오히려 성능을 저하시킬 수 있는 불필요한 데이터로 간주되어 적용하지 않았다. 한편 메타-테스트를 위한 태스크는 본 논문에서 사용한 메타 러닝 모델과 전이 학습 모델에 동일하게 인가되었다.

4. SIMULATION

수신기에 적용 가능한 모델을 구현하기 위해 실제 환경에서 수집한 데이터를 이용하여 데이터셋을 구성할 필요가 있었으므로, 재밍 입사 시의 신호 공분산 배열을 확보하고자 옥외에 3대의 재밍 신호 발생기 및 신호 송신 안테나를 설치한 후 재밍 신호를 송신하였다. 항재밍 알고리즘이 포함되어 신호 공분산 생성을 수행할 GNSS 수신기는 3개 안테나의 중앙에 배치하였으며, 시험 구성도 및 옥외 환경은 Figs. 7, 8과 같다.

Fig. 7에서, 배열 안테나로 입사하는 재밍 신호의 재밍 대 신호 전력 비 (jamming to signal ratio; JSR)는 90 dB로 설정하였으며 배열 안테나와 함께 설치한 센싱 안테나 및 스펙트럼 분석기를 이용하여 이를 검증하였다. 이때 JSR의 값은 본 논문에서 사용한 수신기의 항재밍 신호처리 성능이 신호 유형에 따라 달라지기 시작하며 항재밍 알고리즘의 최적화가 필요해지는 시점인 90 dB를 기준으로 선정하였다. 배열 안테나에서 수신한 재밍 신호는 항재밍 GNSS 수신기로 전달되며, 수신기에서는 항재밍 알고리즘을 위한 공분산을 생성한 후 데이터 케이블을 통해 공분산을 데이터 수집 장치로 전달한다. 이때 표 1에 나타난 메타-학습 데이터셋과 메타-테스트 데이터셋의 클래스마다 50개의 데이터 샘플을 수집하였으며, 메타-학습 데이터셋과 신호 유형이 중복될 경우 동일

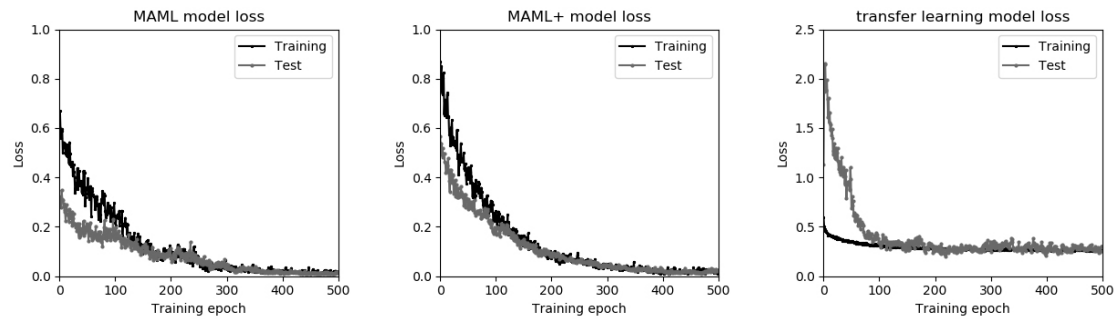


Fig. 9. Training and test loss curves of FSL models.

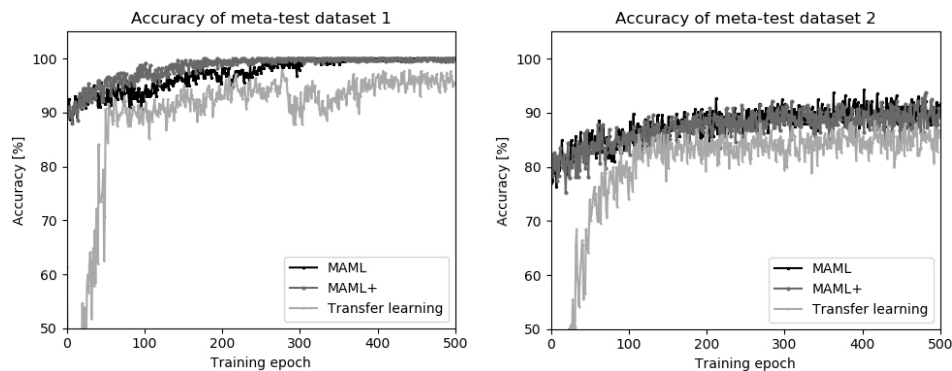


Fig. 10. Training and test accuracy curves of FSL models.

한 데이터를 사용할 수 없으므로 50개의 샘플을 추가적으로 수집하였다.

본 논문에서는 시험을 위해 python 기반의 FSL 시뮬레이터를 설계하였으며, pytorch 라이브러리를 이용하여 2장의 FSL 모델과 3장의 데이터셋 태스크 생성기를 구현하였다. MAML/MAML+ 학습을 위해 매 에피소드마다 메타-학습 데이터셋으로부터 128개의 FSL 태스크로 구성된 샘플 배치를 생성하였으며, 내부 루프의 반복 횟수는 10으로 고정하고 가중치 스텝 크기는 0.01로 설정하였다. 전이 학습 모델의 경우 사전 학습 시에는 데이터와 라벨 쌍으로 구성된 일반적인 입력을 사용하므로 동일한 메타-학습 데이터셋을 이용하여 매 에피소드마다 128개의 입력 데이터로 구성된 샘플 배치를 생성하여 훈련을 진행하였다. 모든 모델은 전부 메타-업데이트를 위한 최적화 함수로 학습률 0.001을 갖는 Adam을 사용하였으며 (Kingma & Ba 2015), Cross-entropy를 손실 함수로 사용하였다.

모델 학습을 위해 메타-학습 데이터셋을 이용한 총 500회의 에피소드 훈련을 진행하였으며, 학습의 성공적인 진행 여부를 확인하기 위하여 메타-학습 데이터셋 및 메타-테스트 데이터셋에 대한 모델 출력을 지속적으로 확인하였다. 본 논문에서는 재밍 신호 식별 성능을 확인하기 위하여 Table 1과 같이 메타-테스트 데이터셋을 두 가지로 구성하였으며, 그 중 메타-테스트 데이터셋 1은 제안한 두 모델이 재밍 신호에 대한 FSL 문제를 효과적으로 해결할 수 있는지 확인하기 위하여 새로운 신호 유형으로만 구성된 바 있다. 따라서 메타-학습 데이터셋과 메타-테스트 데이터셋 1에 대해 본 논문에서 구현한 MAML, MAML+ 및 전이 학습

모델로부터 획득한 손실 그래프를 비교하였으며 결과는 Fig. 9와 같다. 이때 모든 모델의 테스트 손실은 128개의 FSL 태스크로 구성된 메타-테스트 샘플 배치로부터 획득하였다. Fig. 9에서 메타-학습 데이터셋의 손실은 모델의 학습을 위해 사용되지만 메타-테스트 데이터셋의 손실은 모델에 영향을 미치지 않는다. 그럼에도 불구하고 두 손실값이 서로 유사한 값으로 수렴하며 점점 작아진다면 학습이 정상적으로 수행되고 있으며 과적합도 발생하지 않음을 의미한다. 따라서 모델이 정상적으로 학습되었음을 확인할 수 있다.

한편 새로운 신호에 대한 식별 성능뿐만 아니라 기존 신호에 대한 식별 성능 역시 확인하기 위하여 메타-테스트 데이터셋 1과 메타-테스트 데이터셋 2 각각에 대한 모든 모델의 식별 성능을 비교한 결과는 Fig. 10과 같다. Fig. 10으로부터, 본 논문에서 구현한 FSL 모델이 정상적인 학습을 수행하여 에피소드가 증가할수록 새로운 신호 및 기존 신호에 대한 식별 성능이 향상됨을 확인할 수 있다. 또한 메타 러닝 모델인 MAML 및 MAML+의 성능이 에피소드 전체에 걸쳐 전이 학습 모델의 성능보다 상대적으로 우수함을 확인할 수 있다. 최종 성능을 확인하기 위하여 500번의 에피소드 훈련이 종료된 후 메타-테스트 태스크 십만개로 구성된 샘플 배치를 반복 생성하여 식별 성능을 확인한 결과는 Table 2와 같다.

Table 2에서 학습된 FSL 모델이 테스트 시 새로운 유형의 신호에 대해 전부 95% 이상의 식별 성능을 보이는 것을 확인할 수 있다. 이는 새로운 신호에 대한 데이터 하나를 확보했다면 추가적인 학습 없이도 동일한 유형의 신호가 입사될 경우 매우 높은

Table 2. Meta-training and meta-test dataset of MAML/MAML+ and transfer learning.

Dataset	FSL model		
	MAML	MAML+	Transfer learning
Meta-test 1	99.97%	99.91%	96.36%
Meta-test 2	90.34%	89.67%	83.82%

확률로 신호 유형을 판단할 수 있음을 의미한다. 특히 MAML 및 MAML+의 경우, 새로운 신호에 대해 99.9% 이상의 매우 높은 성공률을 보인다. 반면 메타-테스트 데이터셋 2에서는 FSL 모델들의 성능이 상대적으로 저하되어 80%에서 90%의 식별 성공률을 보인다. 이는 학습에 사용된 신호 유형을 사용하였기 때문이 아니라, 메타-테스트 데이터셋 2에서 식별이 필요한 신호 유형의 수가 증가하였으며 그 중 매우 유사한 경향을 가지는 유형들이 존재하기 때문으로 분석할 수 있다.

한편 두 데이터셋에서 전이 학습 모델은 모두 다른 모델에 비해 상대적으로 열화된 성능을 보인다. 이는 데이터의 샘플 수가 부족하여 전이 학습의 모델이 사전 학습을 제대로 수행하지 못했기 때문이다. 공정한 비교와 최적의 성능을 위해서는 대량의 유사한 데이터를 이용하여 충분한 사전 학습을 수행한 특징 추출기를 확보해야 하나, 재밍 신호와 같은 일상적이지 않은 데이터 샘플의 대량 확보는 사실상 불가능하다. 따라서 데이터의 형식이 보편적이지 않으며 제한된 수의 데이터만 존재하는 환경에서는 전이 학습 모델보다 메타 러닝 모델이 보다 효율적이라고 판단할 수 있다.

5. CONCLUSIONS

본 논문에서는 재밍 신호 식별을 위해 전이 학습 및 메타 러닝 기반 식별 알고리즘을 제안하였으며, 실제 환경에서 데이터를 수집하고 python 라이브러리 기반의 시뮬레이터를 구현하여 식별 성능을 확인하였다. 제안한 기법의 인공지능 모델 구조 및 식별 과정이 본문에 간략하게 소개되었으며, 신호 수집 환경과 학습 진행에 따른 결과가 그래프 및 수치로 제시되었다. FSL 문제에서 모델 성능을 판단하기 위한 지표인, 새로운 신호에 대한 식별 성능은 전부 95% 이상을 만족하였으며 항재밍 알고리즘과의 연동을 위해 기 신호 유형까지 식별 범위를 확대할 경우 약 90%의 성능을 보였다. 따라서 제안한 알고리즘을 이용한 재밍 신호 유형의 구분이 유의미한 확률로 가능하며, 항재밍 알고리즘의 성능 향상을 위해 적용할 수 있다.

다만 수신기에서의 실질적인 적용을 위해서는 세 가지 과제가 존재한다. 첫 번째, 새로운 신호 유형이 입사할 경우 이를 클래스로 정의하기 위해서는 사람의 개입이 필요하다는 점이다. 일례로 3FM 신호와 3AWGN 신호의 공분산은 매우 유사한 경향을 보이며 이러한 특징은 Table 2에서 메타-테스트 데이터셋 2를 이용한 식별 성능의 저하로 연결된다. 한편 항재밍 신호처리 관점에서 볼 때, 3FM 신호와 3AWGN의 신호에 대한 대응 방식이 매우 유사하므로 3FM 신호와 3AWGN 신호를 엄밀하게 구분하는 행위에 큰 의미가 없다. 따라서 신호 정의에 대한 사람의 개입이 존재할 경우 3AWGN 신호와 3FM 신호를 하나의 통합된 클래스로

정의할 수 있으며, 이 경우 식별 성능이 향상될 수 있다. 두 번째로는 항재밍 알고리즘 연동에 대한 고려가 필요하다. 항재밍 알고리즘은 재밍 신호의 유형을 입력으로 요구하며, FSL 태스크의 식별 결과를 재밍 유형으로 변환하기 위해서는 각 신호 유형마다 기 확보된 데이터를 서포트 셋으로 사용하여 식별을 진행해야 할 것이다. 이때 서포트 셋과 쿼리 셋의 구성을 어떠한 방식으로 수행할지에 대해 제안된 바가 없으므로 관련 절차에 대한 연구가 진행되어야 한다. 마지막으로, 기 신호를 포함한 식별 성공률이 군 관련 분야에서 기대하는 성능에 미치지 못한다는 과제가 존재한다. 항재밍 알고리즘을 고려한 신호 유형의 재정의 및 모델의 반복적인 최적화를 통해 성능을 향상시킬 수 있는 여지가 충분히 남아 있으나, 머신 러닝의 특성상 최종적인 무결성을 보장하지 못할 가능성이 높다. 따라서 상대적으로 요구 정확도가 낮은, 혹은 제안한 방식을 적용했을 경우 기대 성능이 향상되는 분야에만 본 논문에서 제안한 방식을 적용할 수 있다.

AUTHOR CONTRIBUTIONS

Conceptualization, M. H. Jin; methodology, M. H. Jin; software, M. H. Jin; validation, M. H. Jin and D. Koo; formal analysis, M. H. Jin; investigation, M. H. Jin and D. Koo; resources, K. S. Kim; data curation, K. S. Kim; writing—original draft preparation, M.H. Jin; writing—review and editing, M.H. Jin and D. Koo; visualization, M.H. Jin.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

- Bazec, M. & Dimc, F. 2018, GNSS Jammer detection, classification and spectrum analysis, In *Proceeding of the International Conference on Transport Science*, Portoroz, Slovenia, 14-15 June 2018.
- Fadaei, N. 2016, Detection, characterization and mitigation of GNSS jamming interference using pre-correlation methods, PhD Dissertation, University of Calgary. <https://doi.org/10.11575/PRISM/25598>
- Ferre, R. M., da La Fuente, A., & Lohan, E. S. 2019, Jammer classification in GNSS bands via machine learning algorithms, *Sensors*, 19, 4841. <https://doi.org/10.3390/s19224841>
- Finn, C., Abbeel, P., & Levine, S. 2017, Model-agnostic meta-learning for fast adaptation of deep networks, In *Proceedings of the 34th International conference on machine learning*, Sydney, Australia, 6-11 Aug 2017,

- PMLR, 70, pp.1126-1135. <https://doi.org/10.48550/arXiv.1703.03400>
- Gross, J. N. & Humphreys, T. E. 2017, GNSS spoofing, jamming, and multipath interference classification using a maximum-likelihood multi-tap multipath estimator, In Proceedings of the 2017 International Technical Meeting of the Institute of Navigation, Monterey, California, January 2017, pp.662-670. <https://doi.org/10.33012/2017.14919>
- He, H. & Garcia, E. A. 2009, Learning from imbalanced data, IEEE Transactions on knowledge and data engineering, 21, 1263-1284. <https://doi.org/10.1109/TKDE.2008.239>
- Jin, M. H., Choi, Y., Choi, H. H., & Lee, S. J. 2018, Jammer identification: spectral correlation function and wavelet coherence, Journal of Positioning, Navigation, and Timing, 7, 147-153. <http://doi.org/10.11003/JPNT.2018.7.3.147>
- Jin, M. H., Koo, D. O. R., & Kim, K. S. 2021, Meta-learning Based Few-shot Jamming Signal Classification Technique, 2021 IPNT conference, Gangneung, Korea, 3-5 Nov 2021.
- Kingma, D. P. & Ba, J. 2015, Adam: A method for stochastic optimization, In ICLR, San Diego, CA, USA, 7-9 May 2015. <https://doi.org/10.48550/arXiv.1412.6980>
- Koch, G. 2015, Siamese neural networks for one-shot image recognition, M.S. Dissertation, University of Toronto
- Lee, Y. J., Lee, G. J., & Ra, S. W. 2019, A study on GPS jamming detection using support vector machine, Journal of KIIT, 17, 11-20. <https://doi.org/10.14801/jkiit.2019.17.1.11>
- Moore, T. D. 2002, Analytic study of space-time and space-frequency adaptive processing for radio frequency interference suppression, PhD Dissertation, The Ohio State University.
- Munkhdalai, T. & Yu, H. 2017, Meta networks, In Proceedings of the 34th International conference on machine learning, Sydney, Australia, 6-11 Aug 2017, PMLR, 70, pp.2554-2563
- Pan, S. J. & Yang, Q. 2010, A survey on transfer learning, IEEE Transactions on knowledge and data engineering, 22, 1345-1359. <https://doi.org/10.1109/TKDE.2009.191>
- Ravi, S. & Larochelle, H. 2017, Optimization as a model for few-shot learning, In ICLR, Toulon, France, 24-26 Apr. 2017
- Santoro, A., Bartunov, S., Botvinick, M., Wierstra, D., & Lillicrap, T. 2016, Meta-learning with memory-augmented neural networks, In International conference on machine learning, PMLR, New York, USA, 20-22 Jun 2016, 48, pp.1842-1850. <https://proceedings.mlr.press/v48/santoro16.html>
- Schmidt, R. 1986, Multiple emitter location and signal parameter estimation, IEEE transactions on antennas and propagation, 34, 276-280. <https://doi.org/10.1109/TAP.1986.1143830>
- Settles, B. 2009, Active learning literature survey, Computer Sciences Technical Report 1648, University of Wisconsin-Madison. <http://digital.library.wisc.edu/1793/60660>
- Smith, J. & Abel, J. 1987, Closed-form least-squares source location estimation from range-difference measurements, IEEE Transactions on Acoustics, Speech, and Signal Processing, 35, 1661-1669. <https://doi.org/10.1109/TASSP.1987.1165089>
- Vinyals, O., Blundell, C., Lillicrap, T., Kavukcuoglu, K., & Wierstra, D. 2016, Matching networks for one shot learning, In NIPS, Barcelona, Spain, 5-10 Dec. 2016
- Wang, Y., Yao, Q., Kwok, J. T., & Ni, L. M. 2021, Generalizing from a few examples: A survey on few-shot learning, ACM Computing Surveys, 53, 1-34. <https://doi.org/10.1145/3386252>
- Ward, J. 1994, Space-Time Adaptive Processing for Airborne Radar, Technical Report 1015, Massachusetts Institute of Technology Lincoln Laboratory
- Yoo, S. S. 2020, An improved GNSS jamming classification scheme using convolutional neural network, Journal of Institute of Control, Robotics and Systems, 26, 1016-1027. <http://doi.org/10.5302/J.ICROS.2020.20.0112>



Mi Hyun Jin received the B.S., M.S. and Ph.D. degrees from Chungnam National University. She is a research engineer of DANAM Systems. Her research interests include digital signal processing and software GNSS receiver.



Ddeo Ol Ra Koo received the M.S. degrees from The Graduate School of Advanced Imaging Science, Multimedia & Film, Chung-Ang University. He is a research engineer of DANAM Systems. His research interests include digital signal processing, image processing and software GNSS receiver.



Kang Suk Kim received the B.S. degrees from Dankook University. He is a research engineer of DANAM Systems. His research interests are GNSS receivers and anti-jamming software.