네트워킹을 위한 AI 연구 동향

Trends in AI Researches for Networking

공 정 욱

KiSTi www.kisti.re.kr 한국과학기술정보연구원 Korea Institute of Science and Technology Information

CONTENTS

1. 서론

제4차 산업혁명은 정보통신 기술(ICT)의 융합으로 이루어지는 차세대 산업 혁명이다. 제4차 산업혁명이란 용어는 클라우스 슈바프(Klaus Schwab)가 의장이었던 2016년 세계 경제 포럼(World Economic Forum, WEF)에서 주창된 용어이다. 이 혁명의 핵심은 빅 데이터 분석, 인공지능, 로봇공학, 사물인터넷, 무인 운송 수단(무인 항공기, 무인 자동차), 3차원 인쇄, 나노 기술과 같은 7대 분야에서 새로운 기술 혁신이다[1].

제4차 산업혁명은 물리적, 생물학적, 디지털적 세계를 빅 데이터에 따라서 통합시키고 경제 및 산업 등 모든 분야에 영향을 미치는 다양한 신기술로 설명될 수 있다. 물리적인 세계와 디지털적인 세계의 통합은 O2O를 통해 수행되고, 생물학적 세계에서는 인체의 정보를 디지털 세계에 접목하는 기술인 스마트워치나 스마트 밴드를 이용하여 모바일 헬스케어를 구현할 수 있다. 가상현실(VR)과 증강현실(AR)도 물리적 세계와 디지털 세계의 접목에 해당할 수 있다.

4차 산업혁명의 핵심 속성은 '지능화', '초연결성', '개인화', '융합' 등 4가지가 있다. 인공지능이 등장하여 사물이 지능화되며, 5G를 바탕으로 사람, 기업 등을 넘어 사물까지 실시간으로 연결(IoT)하는 초연결 사회(hyper-connected Society)로 변화하며, 개인맞춤형 제품과 서비스가 가능하며, 산업의 경계가 사라지고 신기술이 전통산업과 융합하여 새로운 일자리 창출이 가능할 것으로 생각된다 [2].

여기서 4차 산업혁명의 핵심은 '인공지능'이다[1]. 인공지능은 데이터를 기반으로 미리 정해진 규칙이 없는 상태에서 데이터로부터 직접 판단 근거를 배우는 알고리즘과 모델을 구축하려고 한다.

현재 인터넷은 통신기술의 급속한 발전과 폭발적인 트래픽의 증가를 경험하고 있다. 기존의 망 정책들은 이러한 변화에 대처할 정도로 정교하지 않은 문제를 갖고 있다. 최근의 인공지능 분야의 발전으로 망 운영자가 더 지능적이고 자율적인 방법으로 망을 설정하고 관리하도록 하는 실행 가능한 접근 방법이 나타나고 있다.

1) 인공지능은 다양한 범위를 포함하지만, 이 문서에서는 머신 러닝과 딥 러닝에 국한해서 기술할 것이다.

이 문서에서는 라우팅 등 망 트래픽 제어와 관련된 네트워킹 분야에서의 머신 러닝/딥 러닝 이슈에 대해 알아보며 혁신적인 네트워킹 알고리즘, 표준, 및 프레임워크를 개발하는데 연구자들에게 도움이 되는 머신 러닝/딥 러닝 관련 연구 동향 및 연구 분야를 소개하고자 한다.

2. 머신 러닝/딥 러닝 개요

2016년 이세돌과 알파고의 바둑 대결은 사람 vs 기계의 대결로써, 기계가 사람을 이기는 것은 시기상조라고 여겼던 전 세계인들을 충격에 빠뜨렸다. 자국의 최고 프로바둑 기사가 기계에 패하는 순간을 생방송으로 본 대한민국 국민은 더 큰 충격을 받았다.

그림 1 딥마인드의 알파고

이후 한국 사회는 그동안 상대적으로 천대받던 인공지능에 대한 본격적인 관심을 두게 되었으며, 국가적으로 많은 연구개발 투자를 수행하고 있다. 학계에서는 인공지능 대학원이 여러 대학에 생겼으며, 기업에서는 그동안 해결하지 못했던 다양한 문제에 인공지능을 적용하여 문제 해결을 했거나 진행 중이다.

머신 러닝은 우리의 일상생활에서 떼려야 뗄 수 없는 존재가 되었다. 예를 들어 다음 홈페이지의 뉴스 노출, 네이버의 검색, youtube 등에서 자동완성, 연관검색어, 음성 인식, 이미지 검색 등 많은 영역에서 머신 러닝이 사용되고 있다.

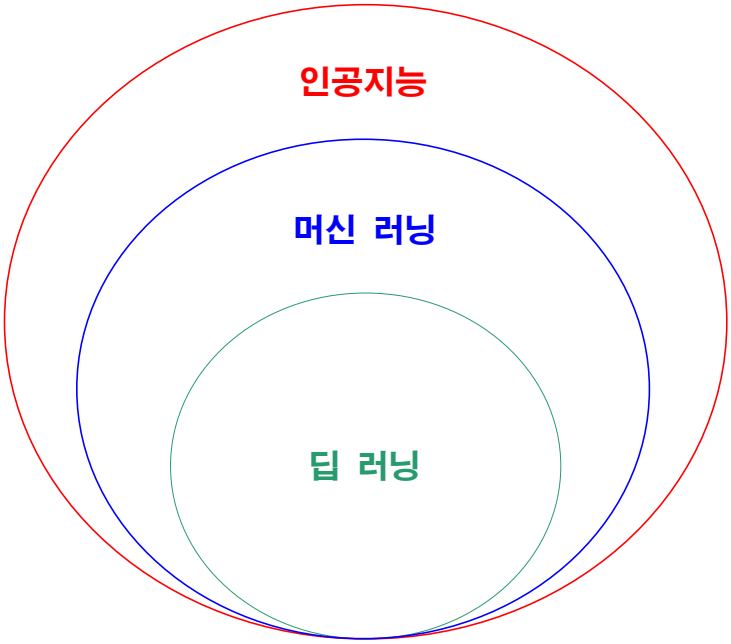

그림 2 인공지능, 머신 러닝 및 딥 러닝의 관계

2.1 머신 러닝이란

인공지능은 지능적 행위를 할 수 있는 컴퓨터와 컴퓨터 소프트웨어, 기계(컴퓨터, 로봇 등)가 보여주는 지능, 인간 지능의 모사(simulation) 등을 말한다. 이처럼 인공지능의 정의는 추상적이며 철학적이다. 지능은 무엇인가? 이 질문에서부터 많은 논란거리가 발생할 수 있으며 철학적 주제이다. 하지만 이 문서에서는 지능을 가진 컴퓨터나 프로그램으로서 인간의 학습 능력, 추론 능력, 언어의 이해 능력 등을 실현하는 (인프라) 기술로 정의하고자 하며, 기계 학습과 딥 러닝은 인공지능이라는 목표를 구현하는 하나의 방법론으로 보는 것이 타당할 것이다.

머신 러닝의 선구자인 Tom Mitchell은 머신 러닝은 '경험을 통해 자동으로 향상되는 알고리즘에 관한 연구 (*the study of computer algorithms that allow computer programs to automatically improve through experience*)'라고 정의했다. 또 널리 인용되고 있는 형식적 정의로써 다음과 같이 이야기하기도 했다: 만약 컴퓨터 프로그램이 특정한 태스크 T를 수행할 대 성능 P만큼 개선되는 경험 E를 보이면 그 컴퓨터 프로그램은 태스크 T와 성능 P에 대해 경험 E를 학습했다고 말할 수 있다(*A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at task in T, as measured by P, improves with experience E.*) [12].

머신 러닝은 특정 업무를 처리하는 컴퓨터 프로그래밍에 관한 접근법이 아니라 '러닝(학습)'이라는 것에 초점이 맞춰져 있다. 머신 러닝이 가능한 기계는 복잡한 알고리즘을 이용해 대량의 데이터를 분석해 그 중 패턴을 인식하고, 그것을 바탕으로 예측을 수행한다. 이 과정에서 인간이 소프트웨어에 특정 명령을 입력할 필요는 없다. 분석 과정에서 만약 치즈 과자를 오렌지로 잘못 인식했다면, 시스템의 패턴 인식 기능은 마치 인간처럼 스스로 오류를 수정하고, 실수로부터 학습하며 정확도를 점점 높여간다. 머신 러닝이 가능한 시스템은 자신의 실수를 토대로 학습하며 패턴 인식 능력을 스스로 향상한다 [3]. 즉 경험을 통해 학습하는 것이다.

여기서 학습(learning)을 했다는 것은 어떤 것일까? 모든 학습 알고리즘은 표현, 평가(evaluation) 및 최적화(optimization)의 세 가지 구성 요소로 되어있다.

표현(representation)은 데이터를 나타내는 모델을 선택한다. 데이터 세트를 생성한 함수는 무엇인가? 이 단계에서 우리는 데이터에 맞는 (나타내는) 모양 (즉, 선형 회귀법에서 선)을 찾으려고 한다. 생성된 데이터에 대해 특정 함수적 형태를 가정하지 않더라도 문제를 구조화할 모델을 결정해야 한다. 입력을 알고리즘이 이해할 수 있는 것으로 바꾸는 표현이 필요하다. 특히 특징 공간(feature space) 또는 상태 공간(state space)에서 입력을 표현하는 방법을 찾는다. 좋은 특징 세트를 사용하면 문제의 실제적 기본 구조에 더 가까워진다. 문제에 대한 모든 중요한 정보를 제공하기 위해 모델에 많은 특징을 포함하리라 생각할 수 있다. 이것은 아마도 과적합(overfilling) 모델로 이어질 것이다. 과적합은 데이터 세트를 생성한 실제 증거 대신 무작위 패턴을 고수하는 모델에 지나지 않는다.

평가(evaluation)는 모델 파라미터에 대해 서로 다른 값을 줬을 때 목적 함수를 최적화한다. 평가/목적 함수는 내부 알고리즘과 외부 모델에 따라 다를 수 있다. 목적 함수는 유틸리티 또는 점수 링 함수라고도 한다. 모델은 알고리즘의 성능 메트릭이다. 함수는 함수의 출력 형태를 포함하여 선택한 표현에 따라 다르다. 학습 중인 모델이 이산적일 때는 분류(classification), 연속적인 출력일 때는 회귀(regression), 함수의 출력이 스칼라일 때는 강화(reinforcement), 함수의 출력이 확률일 때는 확률적(probabilistic)이다.

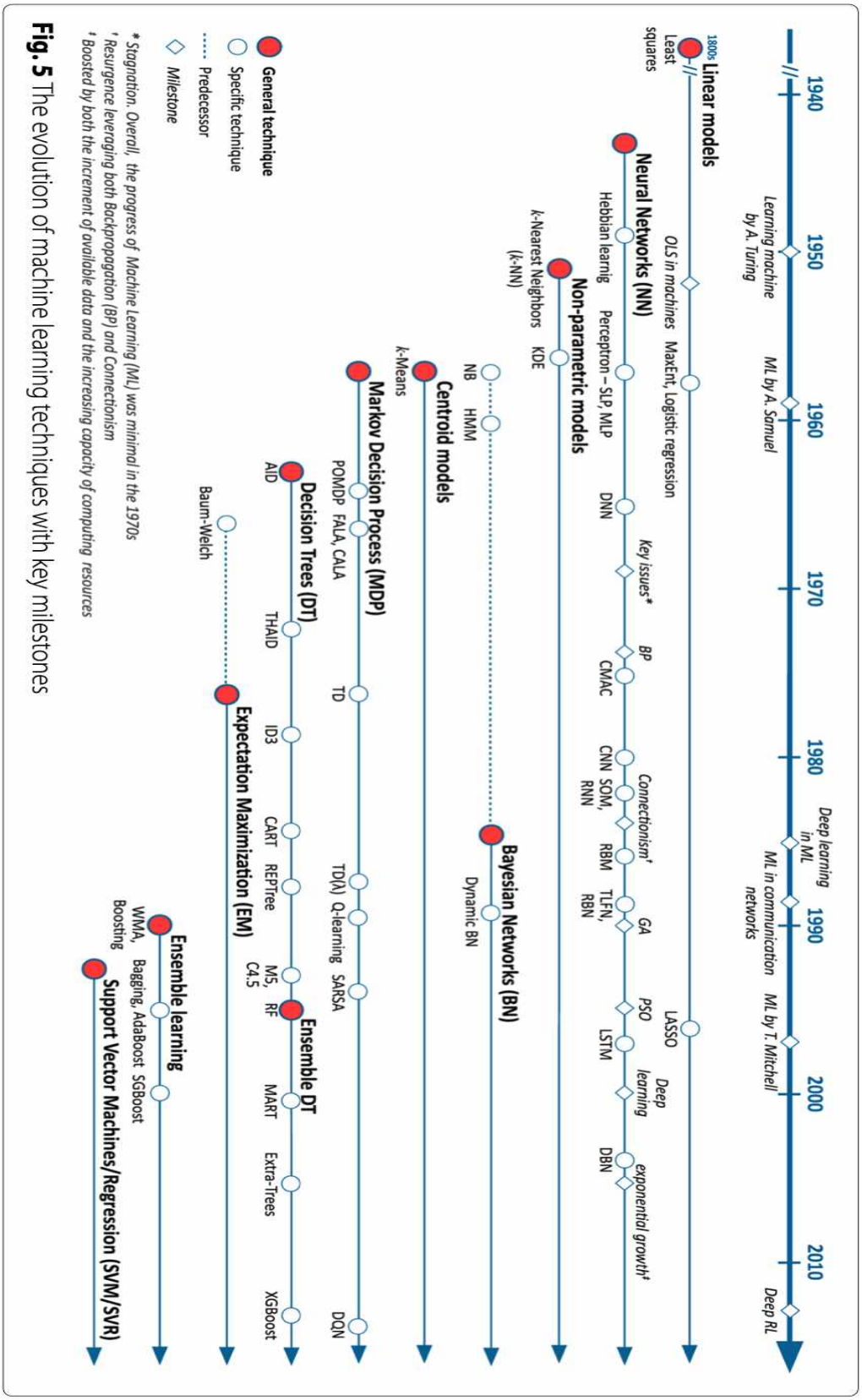

Fig. 5 The evolution of machine learning techniques with key milestones

그림 3 기계 학습 기술의 진화 [4]

최적화(optimization)는 최적화 방법을 사용하여 모델 파라미터를 추정한다. 목적 함수의 최솟값(minims) 또는 최댓값(Maximo)을 찾을 최적화 함수는 무엇일까? 그것이 하는 일은 단순히 모델 파라미터를 계산하고 가장 낮은 오류(minims) 또는 가장 높은 보상(Maximo)을 초래하는 값을 선택하는 것이다. 최적화는 greedy search와 같은 조합, gradient descent와 같은 제약 없는 연속 최적화, 선형 프로그래밍과 같은 제약된 연속 최적화를 기반으로 할 수 있다.

2.2 머신 러닝의 분류

머신 러닝은 지도 학습(supervised learning), 비지도 학습(unsupervised learning), 강화 학습(reinforcement learning) 등 크게 3가지의 유형으로 분류된다. 여기에 준 지도 학습(semi-supervised learning) 등을 유형의 하나로 분류하기도 하지만 위 3가지로 분류하는 것이 큰 흐름인 것으로 판단된다.….

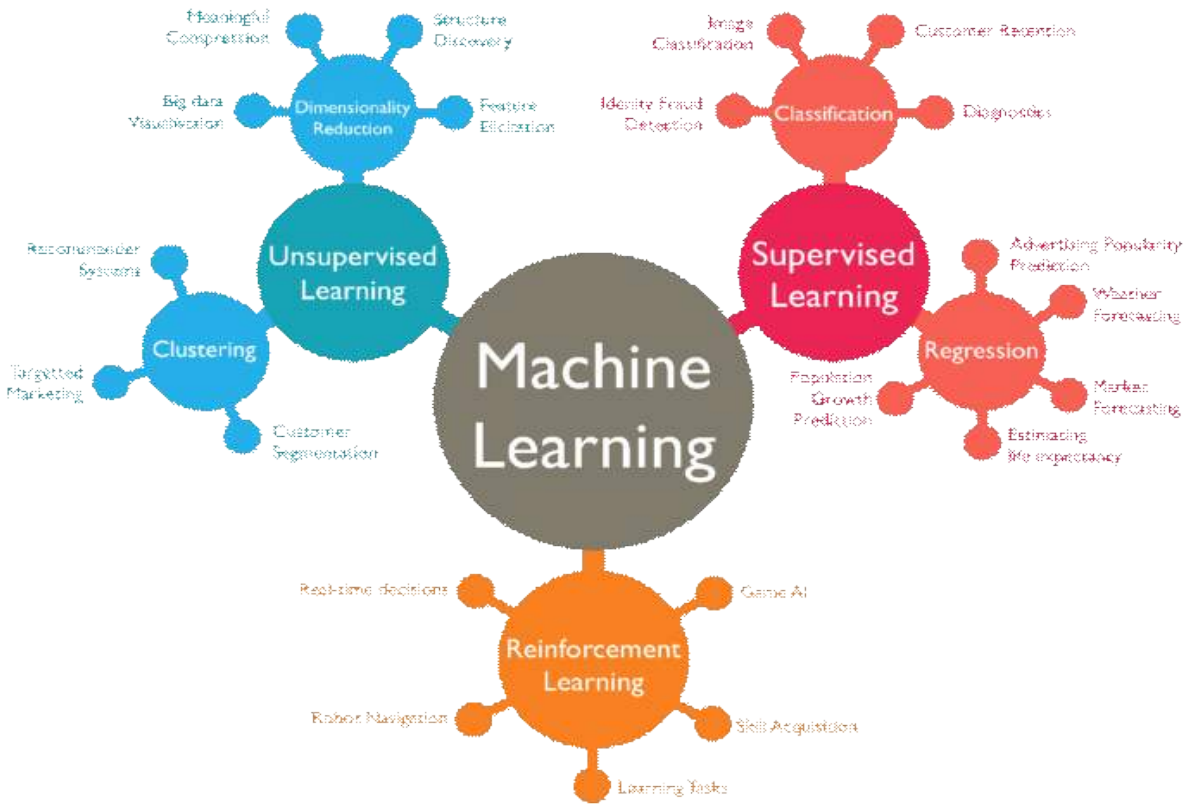

그림 4 머신 러닝의 분류 [5]

학습 데이터 또는 훈련 세트에 붙게 되는 레이블(label)의 유무에 따라 지도 학습과 비지도 학습으로 나뉜다. 레이블은 우리가 분석하고자 하는 학습 데이터의 속성을 정의한 것이다. 사진 속의 사물을 구분하는 작업을 수행한다고 할 때 사진 속의 사

물을 우산, 자동차, 열차 등 데이터에 해당하는 특징을 미리 정해놓은 것은 레이블의 예이다. 이때 레이블이 붙은 사진을 보고 학습을 하는 컴퓨터의 입장에서는 사람의 지도를 받은 것이 되며(지도 학습), 레이블이 없으면 지도를 받은 것이 아니므로 비지도 학습이 된다.….

2.2.1 지도 학습

지도 학습 알고리즘은 훈련 데이터(training data)로부터 하나의 함수를 예측하는 방법이다. 예를 들어, 과거 매출 이력을 이용해 미래 가격을 추산할 수 있다. 지도 학습에는 기존에 이미 분류된 학습 데이터(labeled training data)로 구성된 입력 변수와 원하는 출력 변수가 수반된다. 알고리즘을 이용해 학습용 데이터를 분석함으로써 입력 변수를 출력 변수와 대응시키는 함수를 찾을 수 있다. 이렇게 추론된 함수는 학습용 데이터로부터 일반화(generalizing)를 통해 알려지지 않은 새로운 사례들에 대응하고, 눈에 보이지 않는 상황 속에서 결과를 예측한다.

- 분류(Classification): 어떠한 변수에 영향을 받는 결과를 연속적이지 않은 값들로 나눌 때 사용한다. 이미지에 강아지나 고양이와 같은 레이블 또는 지표(indicator)를 할당하는 경우가 해당한다. 레이블이 두 개인 경우를 '이진 분류'라고 부르며, 범주가 두 개 이상이면 다중 레이블 분류(multi-label classification)라고 부른다.
- 회귀(Regression): 연속적인 값을 예측할 때 문제는 회귀 문제가 된다. 레이블된 학습 데이터를 가지고 특성(feature)과 레이블의 관계를 함수식으로 표현하는 것이 목적이다.
- 예측(Forecasting): 예측 모델은 분류 모델과는 달리 레이블이 달린 학습 데이터를 가지고 특성과 레이블 사이의 상관관계를 함수식으로 표현하게 된다. 따라서 '가', '나', '다'라는 레이블이 달린 데이터를 예측 모델로 지도 학습하였다고 하더라도 분류 모델처럼 결괏값이 반드시 '가', '나', '다'중 하나가 되는 것이 아니라 해당 범위 내의 어떠한 값도 나올 수 있는 것이다. 이처럼 어떠한 값이 결과로 나올지 예상할 수 없으므로, 이를 예측 모델이라 부른다. 이러한 예측 모델은 주가나 환율 분석 등과 같이 연속적인 범위 내의 값에서 그 결괏값을 예측하는 문제에 일반적으로 많이 활용된다.

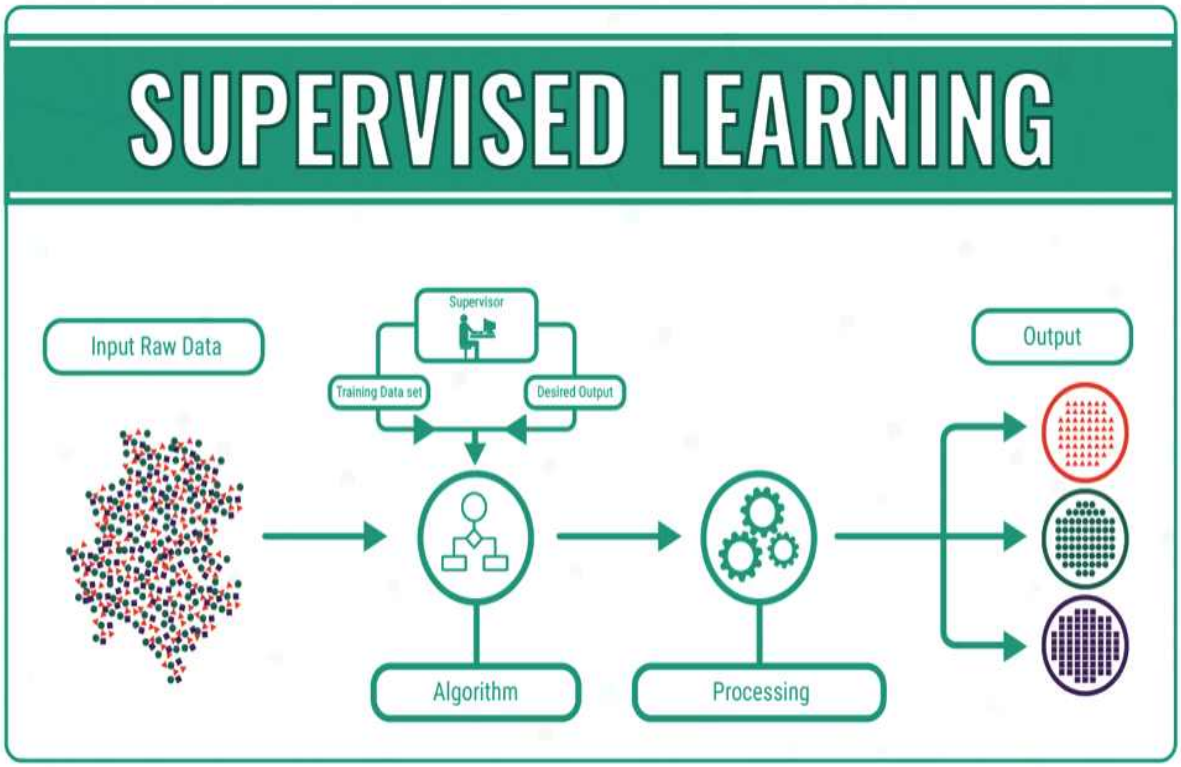

그림 5 지도 학습의 과정 [6]

2.2.2 비지도 학습(unsupervised learning)

비지도 학습은 기계 학습의 일종으로, 데이터가 어떻게 구성되었는지를 알아내는 문제의 범주에 속한다. 이 방법은 지도 학습 혹은 강화학습과는 달리 입력값에 대한 목표치가 주어지지 않는다. 문제는 알려주되 정답까지는 알려주지 않는 학습 방식이다. 즉, 여러 문제를 학습함으로써 해당 데이터의 패턴, 특성 및 구조를 스스로 파악하여, 이를 통해 새로운 데이터에서 일정한 규칙성을 찾는 방법이다.

머신은 클러스터링 구조(clustering structure), 저차원 다양체(low-dimension manifold), 희소 트리 및 그래프(a sparse tree and graph) 등과 같은 데이터의 기저를 이루는 고유 패턴을 발견하도록 설정된다.

비지도 학습은 구체적인 결과에 대한 사전 지식은 없지만, 해당 데이터를 통해 유의미한 지식을 얻고자 할 때 사용되며, 사람도 제대로 알 수 없는 본질적인 문제나

데이터에 숨겨진 특징이나 구조 등을 연구할 때 많이 활용된다.

- 클러스터링(Clustering): 특정 기준에 따라 유사한 데이터 사례들을 하나의 세트로 그룹화한다. 이 과정은 종종 전체 데이터 세트를 여러 그룹으로 분류하기 위해 사용되는데 사용자는 고유한 패턴을 찾기 위해 개별 그룹 차원에서 분석을 수행할 수 있다.
- 차원 축소(Dimension Reduction): 고려 중인 변수의 개수를 줄이는 작업이다. 많은 애플리케이션에서 원시 데이터(raw data)는 아주 높은 차원의 특징을 지니는데, 이때 일부 특징들은 중복되거나 작업과 아무 관련이 없다. 따라서 차원 수(dimensionality)를 줄이면 잠재된 진정한 관계를 도출하기 쉬워진다.

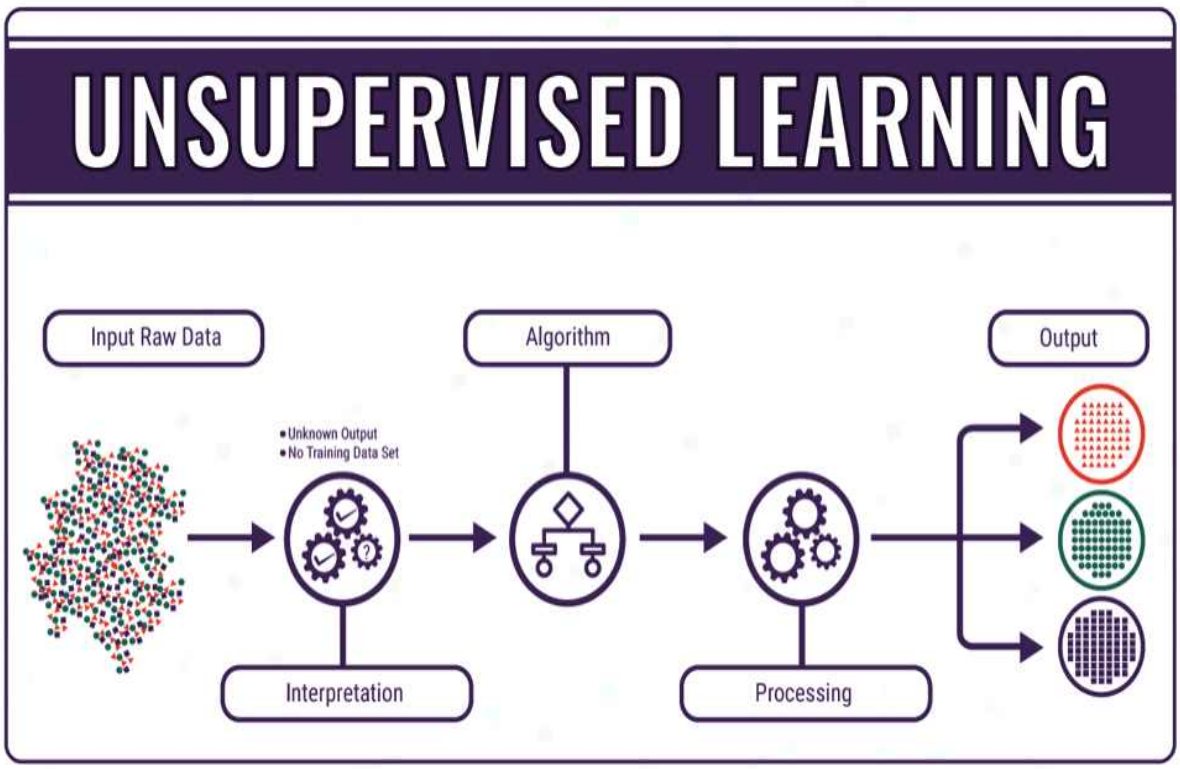

그림 6 비지도 학습의 과정 [6]

2.2.3 강화학습

행동심리학에서 영감을 받았으며, 어떤 환경 안에서 정의된 에이전트가 현재의 상태를 인식하여, 선택 가능한 행동 중 보상을 최대화하는 행동 혹은 행동 순서를 선

택하는 방법이다. 이러한 문제는 매우 포괄적이기 때문에 게임 이론, 제어이론, 운용 과학, 정보 이론, 시뮬레이션 기반 최적화, 다중 에이전트 시스템, 떼 지능, 통계학, 유전 알고리즘 등의 분야에서도 연구된다. 운용 과학과 제어이론에서 강화학습이 연구되는 분야는 "근사 동적 계획법"이라고 불린다. 또한, 최적화 제어이론에서도 유사한 문제를 연구하지만, 대부분 연구가 최적 해의 존재와 특성에 초점을 맞춘다는 점에서 학습과 근사의 측면에서 접근하는 강화학습과는 다르다. 경제학과 게임이론 분야에서 강화학습은 어떻게 제한된 합리성 하에서 평형이 일어날 수 있는지를 설명하는 데 사용되기도 한다 [7].

강화학습 문제를 푸는 것은 최적의 정책 함수를 찾는 것과 같다. 그리고 이 최적의 정책 함수는 불확실한 미래에 얻을 수 있는 보상 함수의 기댓값을 최대로 하는 행동을 매번 고른다. 여기서 눈여겨볼 단어는 '미래'와, '기댓값'이다. 이 두 단어의 의미만 제대로 이해하면 강화학습을 어느 정도 이해했다고 볼 수 있다. 연구자들은 이 강화학습 문제를 풀기 위해서 수학적 모델을 사용하는데, 그것이 바로 마르코프 의사 결정 과정(Markov decision process, MDP)이다 [8].

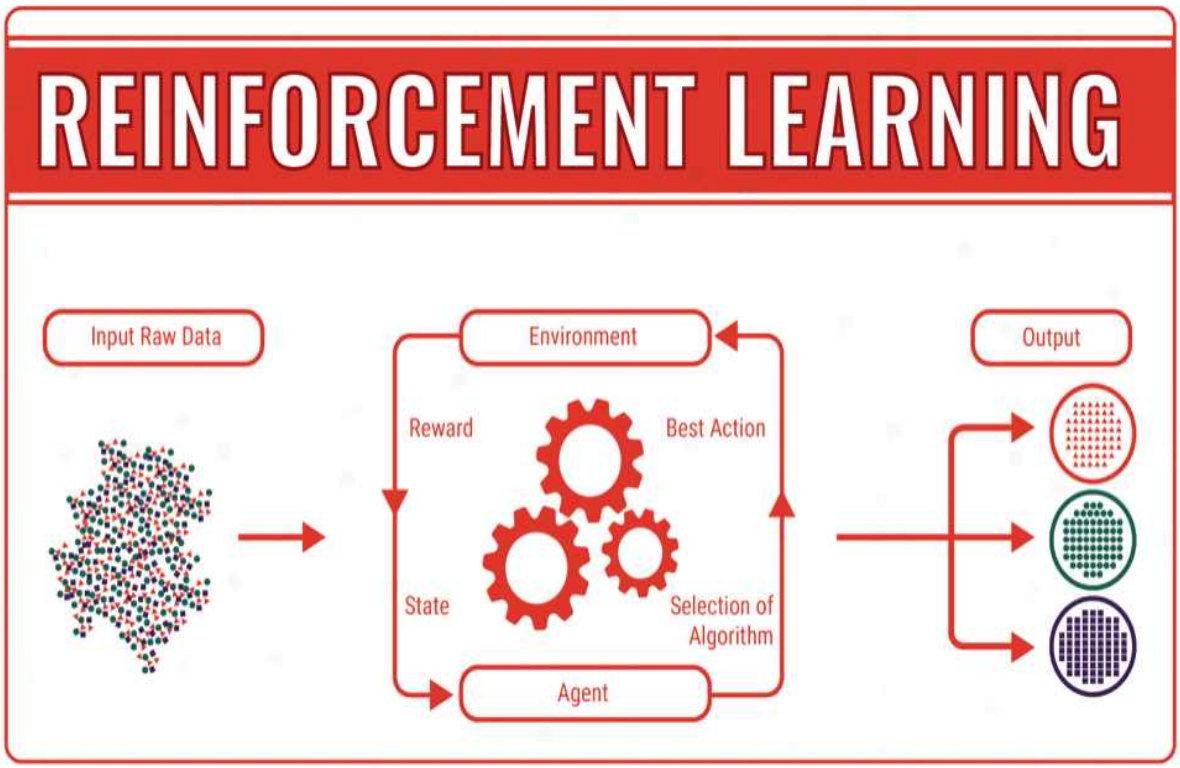

그림 7 강화학습의 과정 [6]

2016년 구글 딥마인드(DeepMind)가 개발한 알파고(AlphaGo)는 바둑을 배운 지 1년 만에 세계 최강의 바둑기사 이세돌을 물리쳐 우리 사회에 남긴 충격은 여전히 남아있다. 2017년 후반 새로운 세대의 소프트웨어로 나온 알파제로(AlphaZero)는 기존 알파고보다 더욱 강력해졌다. 이 알파고와 알파제로에 프로그래밍이 된 학습 모델은 머신 러닝의 학습 모델 중 하나인 강화학습이었다.

알파고는 바둑을 학습하기 위해 가장 먼저 인간의 바둑 경기 데이터베이스를 상대로 학습했다. 이 사전 단계를 통해 심층 신경망 기반의 가치 함수가 적절한 강도로 작동할 수 있게 됐다.

알파고는 다음 학습 단계로 자기 자신과 무수히 많은 경기를 치르면서 결과를 사용해 가치와 정책 네트워크의 가중치를 업데이트했다. 이 과정을 통해 프로그램의 실력이 대부분 인간 바둑기사를 뛰어넘었다.

알파고는 시합 중 각 수마다 그 위치에서 가능한 모든 수에 가치 함수를 적용해 승리로 이어질 가능성의 순위를 매긴다. 그다음 가장 가치가 큰 수를 뒀을 때의 각 바둑판 형태에서 몬테카를로 트리 검색(Monte Carlo tree search) 알고리즘을 실행해 예견한 검색을 기반으로 승리할 가능성이 가장 큰 수를 선택한다. 이 승리 가능성을 사용해 각 수 트리를 검색하는데 투입할 주의력의 가중치를 정한다.

이후의 알파고 및 알파제로 프로그램은 인간 경기 데이터베이스를 상대로 한 학습을 건너뛰었다. 경기 규칙과 강화학습을 제외한 나머지는 모두 빼고 시작한 것이다. 처음에는 임의로 아무 수나 두는 것으로 시작했지만 자신을 상대로 한 수백만 번의 경기를 통해 학습한 후에는 상당한 수준의 경기 능력을 달성했다. 알파고 제로는 3일 만에 100승 0패를 기록하면서 알파고 리(AlphaGo Lee)의 실력을 넘어섰고 21일째에 알파고 마스터(AlphaGo Master) 수준에 도달했으며 40일 후에는 이전의 모든 버전을 추월했다.

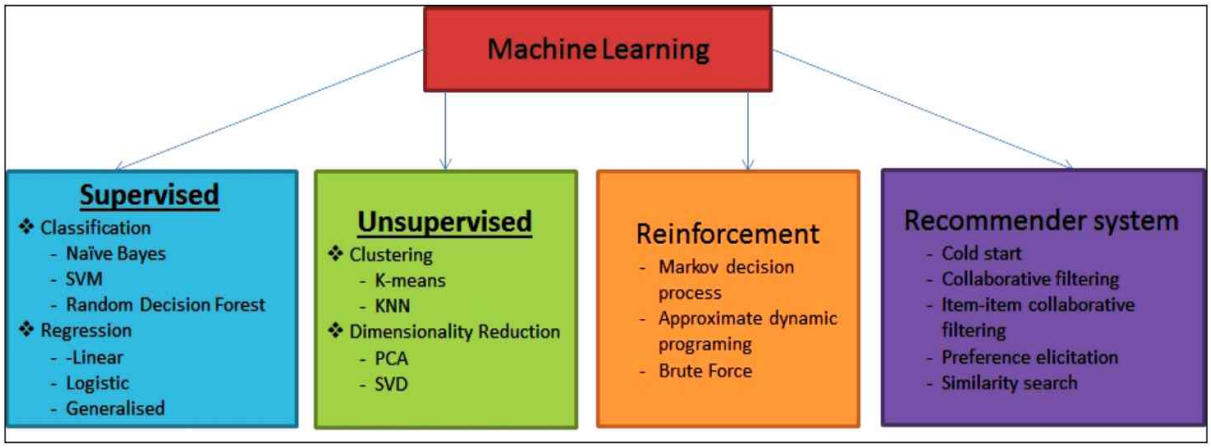

그림 8 머신 러닝 알고리즘 [9]

구분	지도 학습	비지도 학습
경우	예측 모델 생성	고차원 데이터의 분류
검증	교차 검증 수행	없음
입력	레이블 된 데이터	원시 데이터
종류	• 회귀(Regression) • 분류(Classification)	• 군집(Clustering) • 패턴 인식
알고리즘	그림 9 참고	
장점	정확도가 높음	속도가 빠름
단점	학습 데이터의 양이 많아야 하며 시간이 많이 소요됨	학습의 결과에 따른 분류 기준 및 군집 예측 불가
예	주가 예측, 회귀 분석	데이터 마이닝, 스팸 필터

표 1 지도 학습과 비지도 학습의 비교

2.3 딥 러닝이란

딥 러닝(심층 학습)은 머신 러닝의 한 분야로서 기본 층을 겹겹이 연결하여 구성한 신경망(neural network, NN)이라는 모델을 사용하여 연속된 층(layer)으로 표현(representation)을 학습하는 머신 러닝의 한 방식이다. 딥 러닝은 연속된 층에서 점진적으로 의미 있는 표현을 배우는 데 강점이 있으며, 데이터로부터 표현을 학습하는 방식이다. 또한, 딥 러닝은 여러 비선형 변환기법의 조합을 통해 높은 수준의

추상화를 시도한다. 딥 러닝의 '딥'은 연속된 층으로 표현을 학습한다는 개념이며, 딥 러닝 모델에서 층의 개수가 모델의 깊이(depth)가 된다.

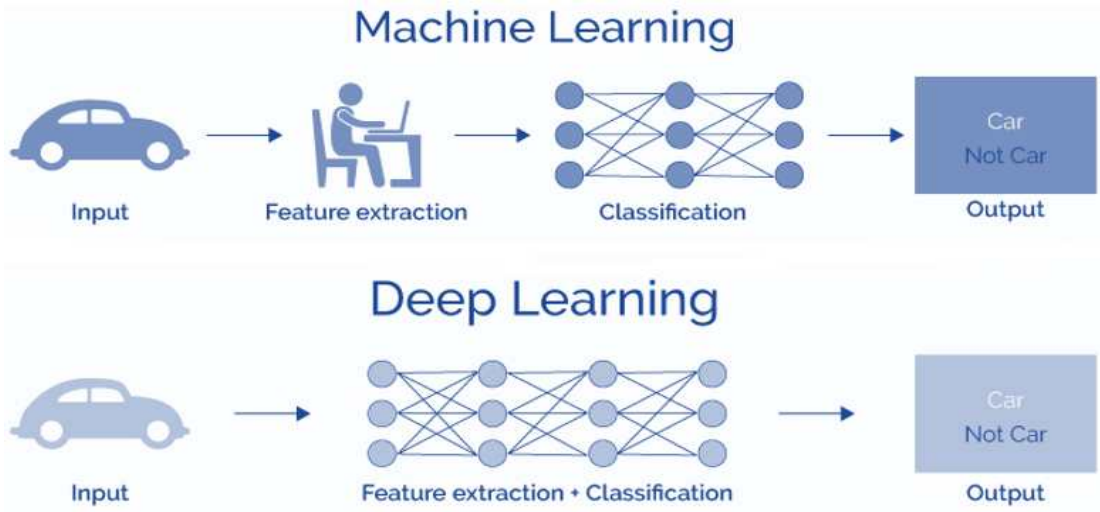

그림 9 머신 러닝과 딥 러닝의 차이

딥 러닝은 deep neural network(DNN)를 이용한 러닝이다. 2~3개의 층을 가지면 shallow learning, 4~10개 층을 가지면 deep learning, 10개 층 이상이면 very deep learning이라고 한다.

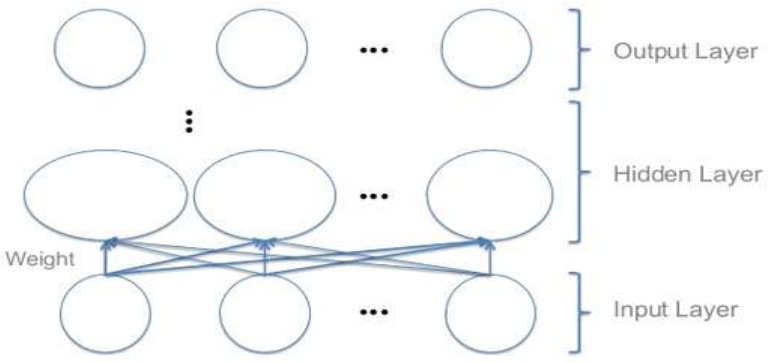

그림 10 Feedforward NN

입력층에 어떤 데이터가 들어오면, 은닉층(hidden layer)에서 여러 연산이 일어난다. 여기서 은닉층이 여러 층 존재하기 때문에 deep이라는 용어를 사용한다. 데이터가 입력층에서 출력층으로 전달되면서 점차 구체화된다. 즉, 중요한 특성은 증폭

되고 반대로 중요하지 않은 특성은 사라진다.

2.3.1 딥 러닝의 일반적인 동작 원리

DNN은 여러 층을 연결하여 '입력'과 '타겟'을 매핑하는 동작을 수행한다. 각 층에서 입력 데이터를 처리하고 가중치(weight)에 저장된다. DNN에서 입력을 타겟에 매핑하기위해 개별 NN에 있는 가중치의 값을 찾는 과정이 학습이다. 이러한 가중치를 찾아내기 위해서는 출력(즉, 예측값)과 실제 타겟의 차이를 측정하는 손실 함수(loss function)를 사용한다. 가중치를 조정하는 과정은 딥 러닝의 역전파(backpropagation)를 이용하며 최적화기(optimizer)가 그 역할을 수행한다.

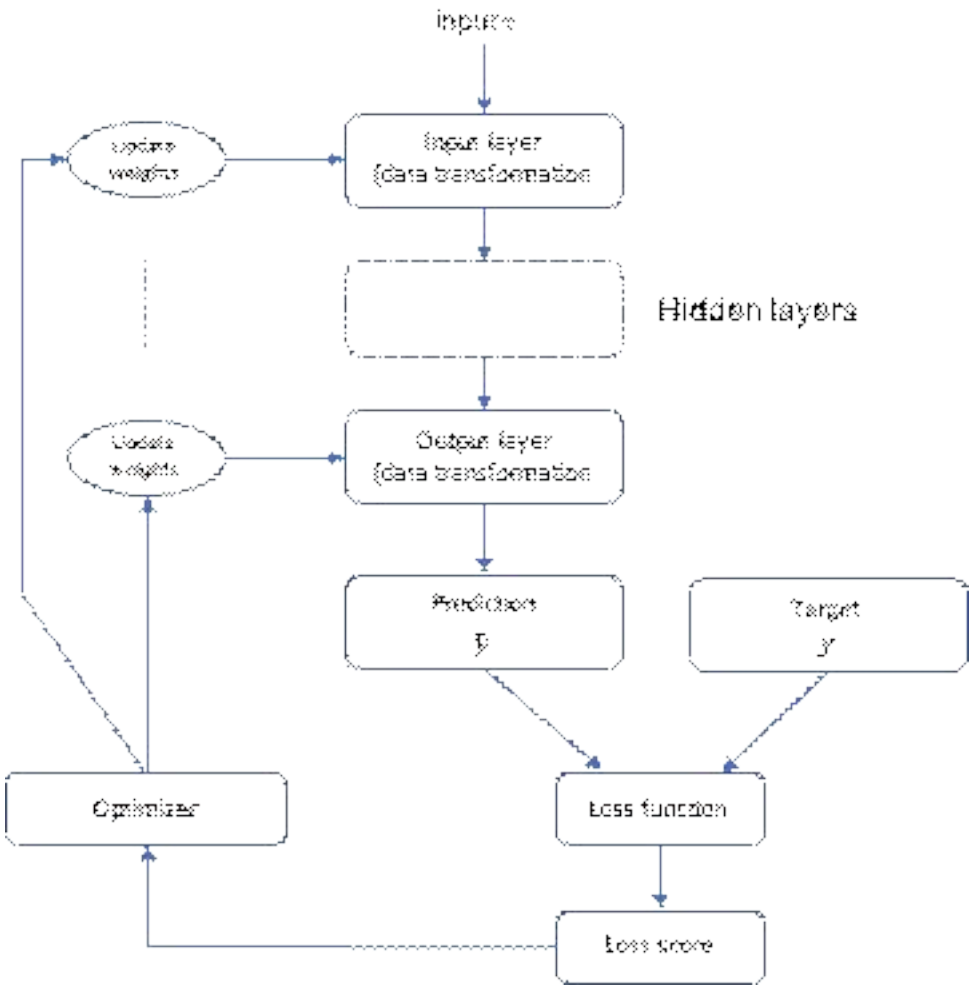

그림 11 딥 러닝 프로세스

트레이닝 초기에는 NN의 가중치가 무작위 값으로 할당되기 때문에 무작위 데이터 변환을 연속적으로 수행한다. 트레이닝 루프를 반복하여 예측값 $\hat{y}$와 타겟 y를 입력으로 하는 손실 함수의 출력을 최소화하는 가중치를 점차 찾아간다.

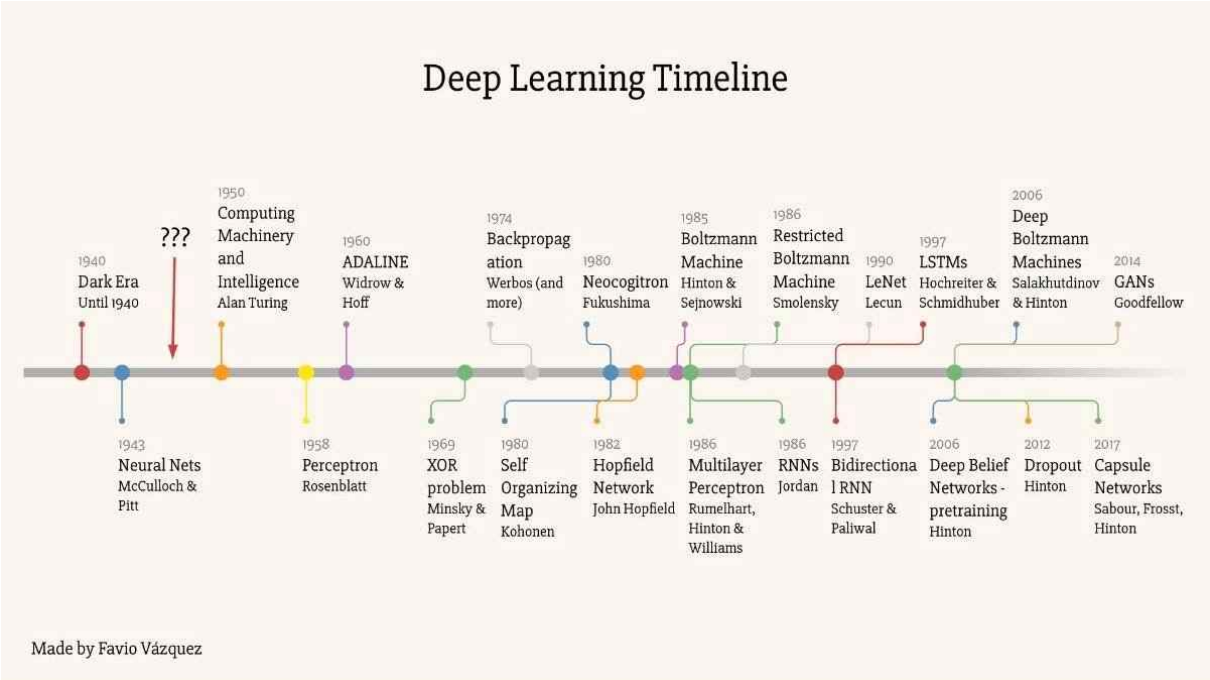

그림 12 딥 러닝의 역사

2.3.2 딥 러닝의 출력층

딥 러닝의 출력층에서는 항등함수(identity function)와 소프트맥스(softmax) 함수를 이용하여 출력값을 얻을 수 있다. 보통 회귀 문제에서는 출력값이 그대로 나오는 항등함수를 사용하는 반면, 분류 문제에서는 출력값의 총합이 1이 되는 소프트맥스 함수를 사용한다.

손실 함수는 실제값과 예측값의 차이를 수치화해주는 함수이다. 이 두 값의 차이 즉, 오차가 클수록 손실 함수의 값은 크고 오차가 작을수록 손실 함수의 값은 작아진다. 회귀에서는 평균 제곱 오차, 분류 문제에서는 크로스 엔트로피를 주로 손실 함수로 사용합니다. 손실 함수의 값을 최소화하는 두 개의 매개 변수인 가중치 와 바이어스를 찾아가는 것이 딥 러닝의 학습 과정이므로 손실 함수의 선정은 매우 중요하다. MSE(Mean Square Error)는 오차 제곱 평균을 의미한다. 연속형 변수를

예측할 때 사용한다.

$$MSE = \frac{1}{N}\sum_{n=1}^{N}(y_n - \hat{y_n})^2.$$

크로스엔트로피는 낮은 확률로 예측해서 맞추거나, 높은 확률로 예측해서 틀리는 경우 손실이 더 크다.

$$CrossEntropy = -\sum_{n} y_n \log \hat{y_n}.$$

딥 러닝의 출력층에서 분류 알고리즘으로 사용되는 SVM(Support Vector Machine)과 소프트맥스에 대해 알아보자. 여기서 y_i는 i번째 타겟(정답 레이블) 값, s_{y_i}는 y_i 값에 대한 score 값, E_i는 손실 함수이다. SVM에 대한 손실 함수는

$$E_i = \sum_{y_j \neq y_i} \max(0, s_{y_j} - s_{y_i} + 1)$$

이며, 소프트맥스에 대한 손실 함수는

$$E_i = \frac{e^{s_{y_i}}}{\sum_{n} e^{s_{y_n}}}$$

이다. 분류 시 SVM은 가장 작은 E_i 값을 선택하고, 소프트맥스는 큰 E_i 값을 선택한다. 소프트맥스 함수의 출력은 0에서 1.0 사이의 실수이다. 또한, 소프트맥스 함수의 출력 총합은 1이다. 출력 총합이 1이 된다는 점은 소프트맥스 함수의 중요한 성질이다. 이러한 성질 때문에 함수의 출력을 "확률"로 해석하여 분류할 수 있는 것이다.

2.3.3 역전파(Backpropagation)

역전파(back propagation)는 출력층에서 계산된 에러값이 역방향으로 즉 출력층에서 각 층으로 전파되면서 각 층에 있는 가중치가 보정되는 과정, 즉 학습 과정을 수행하는 것이다. 주로 경사감소법(gradient descent)이 사용되지만, 경사감소법은 항상 전역 최솟값(global minimum)을 찾는다고 보장할 수 없다. 극솟값이 두 개 이상 존재하는 함수에 대해 가장 작은 최솟값을 찾는다고 할 수 없다. 알고리즘이 단순히 기울기가 작아지는 방향으로 움직이는 것이기 때문에, 시작점에 따라 결과가 달라질 수 있다.

경사감소법은 아래로 볼록한 2차 함수인 E(손실 함수, 목적 함수 등)를 최소화하는 파라미터(가중치)를 구하는 방법이다. 즉 다음 수식의 E를 최소화하는 가중치를 찾는 것이다.

$$E = \frac{1}{2}\sum_{i}^{N}(\text{label} - \text{prediction})^2$$

여기서 손실 함수를 계산할 때 전제 Train-Set을 사용하는 것을 Batch Gradient Descent라고 한다. 그러나 이렇게 계산하면 한번 단계를 내디딜 때, 전체 데이터에 대해 손실 함수를 계산해야 하므로 너무 많은 계산량이 필요하다. 이를 방지하기 위해 보통은 Stochastic Gradient Desenct(SGD)라는 방법을 사용한다. 이 방법에서는 손실 함수를 계산할 때, 전체 데이터(Batch) 대신 일부 데이터의 모음(Mini-Batch)을 사용하여 손실 함수를 계산한다. Batch Gradient Descent보다 다소 부정확할 수는 있지만, 계산 속도가 훨씬 빠르므로 같은 시간에 더 많은 단계를 갈 수 있으며, 여러 번 반복할 경우 일괄 처리한 결과로 수렴한다. 또한, Batch Gradient Descent에서 빠질 극솟값(local minima)에 빠지지 않고 더 좋은 방향으로 수렴할 가능성도 크다. 여기에 더해 SGD를 변형시킨 여러 알고리즘을 활용하면 훨씬 좋은 성능을 낼 수 있고, 변형된 알고리즘으로 Naive Stochastic Gradient Descent, Momentum, NAG, Adagrad, AdaDelta, RMSprop 등이 있다.

구분	Batch Gradient Descent (BGD)	Mini-Batch Gradient Descent (MBGD)	Stochastic Gradient Descent (SGD)
활용	• 데이터 세트 규모가 작고 redundancy가 작을 경우	• 데이터 세트 규모가 크고 redundancy가 많은 경우	• MBGD와 유사, 빠른 계산을 원할 경우
장점	• 최솟값에 수렴 • 병렬 프로그래밍	• BGD와 SGD 장점 보유 • 배치 크기=50~256 • GPU 효용성 증가	• 빠른 계산 속도 • 적은 메모리 용량 • No Redundancy • 극솟값 탈출
단점	• 메모리 용량 제한 • 계산 시간 • Redundancy(반복 계산)	• 최적 미니 배치 크기 결정 필요 • BGD보다 정확도 낮음	• 최솟값에 수렴이 늦음 • one-by-one 계산 (GPU 활용률이 낮음)

표 2 BGD vs MBGD vs SGD

2.3.4 딥 러닝이 유행하는 이유

딥 러닝이 주목받는 것은 다음 세 가지 기술적인 힘이 큰 역할을 했다.

- 하드웨어
- 데이터셋과 벤치마크
- 알고리즘 향상

◯ 하드웨어

CPU의 속도가 급속히 빨라지고 하나의 칩 내에 여러 개의 코어를 집적할 수 있게 되었다. 그렇기에 작은 딥 러닝 모델의 경우에는 노트북에서도 돌릴 수 있게 되었다. 하지만 컴퓨터 비전이나 음성 인식에서 사용되는 일반적인 딥 러닝 모델들은 노트북보다 수에서 수십 배의 계산 능력이 필요하다. 이런 상황에서 2000년대 게임 그래픽 성능 개발을 위한 대용량 고속 병렬 칩(그래픽 처리장치 GPU)이 발전하였고, GPU 제품을 위한 프로그래밍 인터페이스 CUDA가 출시되었다. 물리 모델링을 시작으로 신경망까지 병렬화가 가능해진 것이다.

게임용 GPU인 NVIDIA TITAN X는 6.6 테라플롭스의 단정도 연산 성능을 제공한다. 이는 초당 6.6조 개의 float 32 연산을 수행한다(PS에서 1초에 2~3억 연산을 가정하고 풀었는데 엄청난 속도이다). 큰 회사에서는 딥 러닝을 위한 GPU 수백 개로 딥 러닝 모델을 훈련시킨다.

이에 더하여 구글은 2016년에 텐서 처리장치 프로젝트를 공개했다. 이 칩은 심층 신경망을 실행하기 위해 완전히 새롭게 설계한 것으로 최고 성능을 가진 GPU보다 10배 이상 빠르고 에너지 소비도 더 효율적이다. (2017에 발표한 TPU는 180 테라플롭스입니다.)

◯ 데이터

데이터가 생산되는 속도가 너무 빠르고 그 양 또한 방대하다. 저장 장치의 발전, 데이터셋을 수집하고 배포할 수 있는 인터넷의 성장은 머신 러닝에 필요한 데이터들을 마련할 수 있는 환경을 만들어주었다. 비디오에는 유튜브, 자연어에는 위키피디

아, 이미지는 플리커 등 다양한 데이터가 존재한다. 1400만 개의 이미지를 1000개의 범주로 구분한 ImageNet도 빼놓을 수 없는 데이터셋이다.

◯ 알고리즘

- 활성화 함수
- 가중치 초기화 방법
- 최적화 방법

위의 방법 등은 더 많은 층의 딥 러닝을 가능하게 만들었다. 이제는 층의 깊이가 수천 개인 모델을 처음부터 훈련시킬 수 있다.

2.3.5 딥 러닝의 활용 분야

- 이미지 분류
- 음성/필기/사물 인식
- TTS (Text to Speech)
- 번역기
- 의료 산업 : 신규 후보물질 발굴, 분자 모델링, 대사·독성 예측 등
- 디지털 비서
- 자율주행 차
- 광고 타게팅
- 웹 엔진 결과
- 자연어 질의 대답 능력
- 바둑 등

3. 네트워킹을 위한 머신 러닝/딥 러닝

최근 네트워크는 IoT, 클라우드, 4G/5G 모바일 네트워크, 빅 데이터, AI 기술 등과 결합하여, '초연결(hyper-connected) 데이터 중심 사회'와 COVID-19로 인한 비대면(untact) 사회로의 변화의 중심에 있다. 특히, 과학 분야에서는 빅 데이터 사이언스의 출현으로 네트워크는 고성능 컴퓨팅 서비스와 융합된 서비스가 더욱 중요하게 되었다.

현재 네트워크 분야에서는 타 분야와 마찬가지로 AI를 이용하여 네트워크상에서 발생하는 다양한 이슈를 해결하고자 모색 중이다. 대표적으로, 시계열(time series) 또는 비시계열(non-time series) 기반 트래픽 예측, 페이로드/호스트/플로우 특징 기반 트래픽 분류, 트래픽 라우팅, 혼잡 제어(congestion control), 자원 관리(수락 제어, 자원 할당 등), 오류 관리(fault management), QoS와 QoE 관리, 네트워크 보안, 네트워크 운영 및 관리 자동화 등의 분야가 있다.

3.1 MLN(Machine Learning for Networking)의 워크플로우 [11]

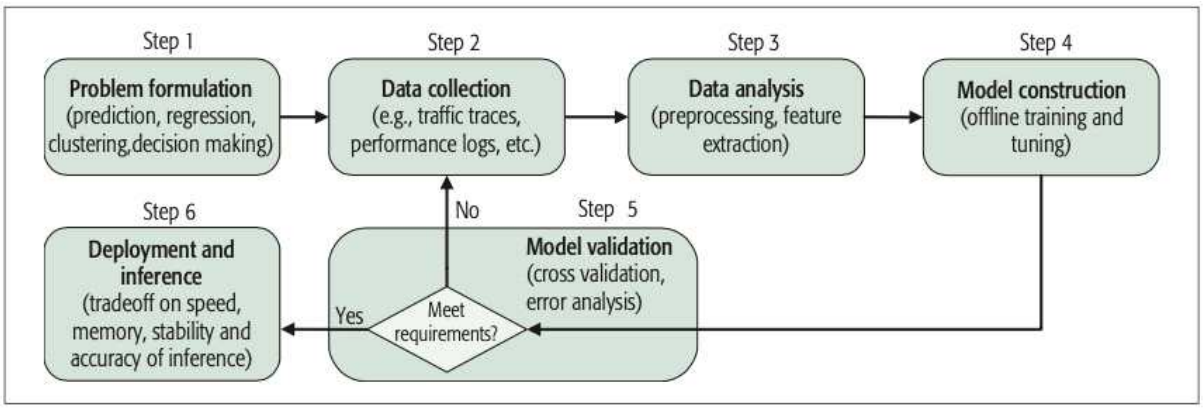

그림 13 MLN의 전형적 워크플로우

그림 13는 문제 공식화(problem formulation), 데이터 수집, 데이터 분석, 모델 구성, 모델 유효성 검사, 배포 및 추론을 포함하여 네트워크 분야에서 머신 러닝을 적용하기 위한 기본 워크플로우를 보여준다. 이 단계들은 서로 독립적이지 않고 내부적으로 서로 관계가 있다. 네트워크 문제는 여전히 머신 러닝이 역할을 수행할 수

있는 애플리케이션이므로 이 워크플로우는 머신 러닝을 위한 기존 워크플로우와 매우 유사하다. 이 절에서는 MLN 워크플로우의 각 단계를 대표적인 사례와 함께 설명한다.

문제 공식화 : 기계 학습의 훈련 과정은 종종 시간과 비용이 많이 들기 때문에 MLN의 첫 번째 단계에서 문제를 올바르게 추상화하고 공식화하는 것이 중요하다. 대상 문제는 분류, 클러스터링 및 의사 결정과 같은 기계 학습 범주 중 하나로 분류될 수 있다. 이를 통해 수집할 데이터의 종류와 양과 선택할 학습 모델을 결정하는 데 도움이 된다. 부적절한 문제 추상화는 부적합한 학습 모델을 제공하여 만족스럽지 못한 학습 성능을 초래할 수 있다. 예를 들어 라이브 스트리밍을 위한 최적의 QoE(체감 품질)를 예측 기반 문제가 아닌 실시간 탐험-활용 프로세스(exploration-exploitation process)로 캐스팅하여 애플리케이션 특성과 잘 일치하는 것이 좋다.

데이터 수집 : 이 단계의 목표는 편견 없이 많은 양의 대표적인 네트워크 데이터를 수집하는 것이다. 네트워크 데이터 (예 : 트래픽 추적 및 성능 메트릭이 있는 세션 로그)는 애플리케이션 요구사항에 따라 서로 다른 네트워크 계층에서 기록된다. 예를 들어, 트래픽 분류 문제는 종종 해당 애플리케이션 클래스로 레이블이 지정된 패킷 레벨의 추적을 포함하는 데이터셋이 필요하다. MLN의 맥락에서 데이터는 종종 두 단계로 수집된다. 오프라인 단계에서 충분한 고품질 기록 데이터를 수집하는 것은 데이터 분석 및 모델 학습에 중요하다. 온라인 단계에서 실시간 네트워크 상태 및 성능 정보는 종종 학습 모델의 입력 또는 피드백 신호로 사용된다. 새로 수집된 데이터를 저장하여 모델 적응을 위한 기록 데이터 풀을 업데이트할 수도 있다.

데이터 분석 : 모든 네트워크 문제에는 고유한 특성이 있으며 여러 요인의 영향을 받지만 몇 가지 요인(예 : 기능)만이 대상 네트워크 성능 메트릭에 가장 큰 영향을 미친다. 예를 들어, RTT와 ACK의 도착 간 시간(inter-arrival time)은 TCP 혼잡 윈도우의 최적 크기를 선택하는데 중요한 특징이 될 수 있다. 학습 패러다임에서 적절한 특징을 찾는 것이 데이터의 잠재력을 완전히 발휘하는 열쇠이다. 이 단계는 머신 러닝 커뮤니티에서 특징(feature) 엔지니어링 프로세스로 간주할 수 있는 과거 데이터 표본을 분석하여 네트워크 문제의 효과적인 기능을 추출하려고 시도한다. 특징 추출 전에 정규화, 이산화 및 손실된 값 채우기와 같은 프로세스를 통해 원시

데이터를 사전 처리하고 정리하는 것이 중요하다. 정리된 데이터에서 특징을 추출하려면 대상 네트워크 문제에 대한 도메인별 지식과 통찰력이 필요한 경우가 많다. 이는 어렵고 시간이 오래 걸린다. 따라서 어떤 경우에는 딥 러닝이 특징 추출을 자동화하는 데 도움이 되는 좋은 선택이 될 수 있다.

모델 구성 : 모델 구성에는 모델 선택, 훈련 및 조정이 포함된다. 데이터 세트의 크기, 네트워크 시나리오의 전형적인 특성, 문제 범주 등에 따라 적절한 학습 모델 또는 알고리즘을 선택해야 한다. 예를 들어, 정확한 처리량(throughput) 예측은 인터넷 비디오의 비트 전송률 조절을 향상할 수 있으며 상태 저장 처리량의 동적 패턴으로 인해 예측을 위해 Hidden-Markov 모델이 선택될 수 있다. 그런 다음 이력 데이터를 사용하여 하이퍼 파라미터 조정으로 모델을 학습시키므로 오프라인 단계에서 오랜 시간이 걸린다. 매개 변수 조정 프로세스에는 여전히 충분한 이론적 지침이 부족하며 종종 허용 가능한 매개 변수를 찾거나 개인적인 경험에 따라 조정하기 위해 넓은 공간에서 검색해야 한다.

모델 검증 : 오프라인 검증은 학습 알고리즘이 충분히 잘 작동하는지 평가하기 위해 MLN 워크플로우에서 없어서는 안될 단계이다. 이 단계에서 교차 검증은 일반적으로 모델이 과적합(overfitting)인지 과소 적합(underfitting)인지를 보여주기 위해 모델의 전체 정확도를 테스트하는 데 사용된다. 이는 모델을 최적화하는 방법에 대한 좋은 지침을 제공한다 (예 : 과적합이 있을 때 데이터 볼륨 증가 및 모델 복잡성 감소). 잘못된 표본을 분석하면 오류의 원인을 찾아 모델과 특징이 적절한지 또는 데이터가 문제에 대해 충분히 대표되는지를 판단하는 데 도움이 된다. 오류 원인에 따라 이전 단계의 절차를 다시 수행해야 할 수 있다.

배포 및 추론 : 운영 네트워크 환경에서 학습 모델을 구현할 때 몇 가지 실질적인 문제를 고려해야 한다. 종종 계산이나 에너지 자원에 제한이 있고 응답 시간에 대한 요구사항이 있으므로 실제 네트워크 시스템의 성능을 위해서는 정확도와 오버헤드 사이의 균형이 중요하다. 또한, 기계 학습은 종종 best-effort 방식으로 작동하며 성능 보장을 제공하지 않으므로 시스템 설계자는 내결함성(fault tolerance)을 고려해야 한다. 마지막으로, 실제 응용 프로그램은 종종 학습 시스템이 실시간 입력을 받고 추론을 얻고 해당 정책을 온라인으로 출력하도록 요구한다.

3.2 MLN 연구 동향[2][4]

3.2.1 트래픽 예측

네트워크 트래픽 예측은 오늘날 점점 복잡해지고 다양해지는 네트워크의 운영 및 관리에서 핵심적인 역할을 한다. 이는 미래의 트래픽을 예측하는 것을 수반하며 전통적으로 시계열 예측 (time series forecasting, TSF)을 통해 해결되었다. TSF의 목적은 미래 트래픽 볼륨과 이전에 관찰된 트래픽 볼륨 간의 정확한 상관관계를 도출할 수 있는 회귀 모델을 구성하는 것이다.

트래픽 예측을 위한 기존 TSF 모델은 통계 분석 모델과 지도(supervised) ML 모델로 광범위하게 분해될 수 있다. 통계 분석 모델은 일반적으로 일반화된 자기 회귀 통합 이동 평균 (auto-regressive integrated moving average, ARIMA) 모델을 기반으로 구축되는 반면 트래픽 예측을 위한 학습 대부분은 지도 NN을 통해 수행된다. 일반적으로 ARIMA 모델은 TSF에 대해 널리 사용되는 접근 방식으로, 자기 회귀 (AR) 및 이동 평균 (MA) 모델에 나란히 적용되어, 차이가 있고 비유동적인 데이터에 대한 자동 회귀를 수행한다. 그러나 네트워크의 급속한 성장과 네트워크 트래픽의 복잡성이 증가함에 따라 기존 TSF 모델이 손상되어 보다 고급 ML 모델이 출현한다. 최근에는 트래픽 볼륨이 아닌 플로우의 특징을 사용하여 오버헤드를 줄이고 트래픽 예측의 정확성을 높이기 위한 노력이 이루어졌다.

2) 이 절은 참고문헌 [4] 의 내용을 발췌하여 오류를 수정하고 요약 정리한 것이다.

응용(방법)	ML 기술	데이터셋	특성(feature)	출력
단대단 대역폭 가용성 예측(TSF)	지도: MLP-NN	NSF TeraGrid 데이터셋	과거 10~30초 동안 max, min, avg 부하	미래의 단대단 가용 대역폭
링크 부하 및 트래픽 양 예측(TSF)	지도: NNE	SNMP 트래픽 데이터	트래픽 양	예상 트래픽 양
링크 부하 예측(TSF)	지도: SVR	ISP의 POP에서 수집한 인터넷 트래픽	τ 동안 관찰된 링크 부하	예상 트래픽 양
네트워크 트래픽 예측(TSF)	지도: MLP-NN	1000포인트 데이터셋	과거 측정값	예상 트래픽 양
네트워크 트래픽 예측(TSF)	지도: MLP-NN	2주간의 시간마다 측정한 트래픽	매시간 트래픽 양	내일 시간당 예상 트래픽 양
데이터센터 사이의 트래픽 양 예측(회귀)	지도: MLP-NN	6주간의 데이터센터 간 트래픽	시간 및 주파수 특성을 추출하기 위한 레벨-N wavelet 변환	$k \times 30$s 뒤 예상 트래픽 양
플로우 통계 기반 미래 트래픽 양 예측(회귀)	지도: KBR, LSTM-RNN	24주간 매시간 5분 동안 수집한 트래픽 양 및 플로우 수	플로우 수	예상 트래픽 양
초기 플로우 크기 예측 및 elephant 플로우 탐지(분류)	지도: GPR, oBMM, MLP-NN	300만 이상의 플로우를 갖는 3개 대학의 네트워크 데이터셋	src IP, dst IP, src port, dst port, protocol	플로우 크기 클래스, elephant vs non-elephant

표 3 트래픽 예측 연구 동향

3.2.2 트래픽 분류

트래픽 분류는 네트워크 운영자가 광범위한 네트워크 운영 및 관리 활동을 수행하는 데 필수적이다. 여기에는 용량 계획, 보안 및 침입 감지, QoS 및 서비스 차별화, 성능 모니터링 및 자원 프로비저닝이 포함된다. 예를 들어, 엔터프라이즈 네트워크의 운영자는 비즈니스에 중요한 애플리케이션에 대한 트래픽의 우선순위를 지정하고, 이상 감지를 위해 알려지지 않은 트래픽을 식별하거나, 다양한 애플리케이션 성능 및 자원 요구사항을 충족하는 효율적인 자원 관리 체계를 설계하기 위해 워크로드 특성화를 수행하고자 할 수 있다.

트래픽 분류에는 네트워크 트래픽을 사전 정의된 관심 클래스에 정확하게 연결하는 기능이 필요하다. 이러한 관심 클래스는 애플리케이션 클래스 (예 : HTTP, FTP, WWW, DNS 및 P2P), 애플리케이션 (예 : Skype, YouTube 및 Netflix) 또는 서비스 클래스일 수 있다. 예를 들어 QoS 기반 서비스 클래스는 동일한 QoS 요구 사항을 가진 모든 애플리케이션 또는 애플리케이션 클래스를 포함한다. 따라서 다르게 동작하는 애플리케이션이 동일한 서비스 클래스에 속할 수 있다.

일반적으로 네트워크 트래픽 분류 방법론은 포트 번호, 패킷 페이로드, 호스트 동작 또는 플로우 특징을 활용하는 네 가지 광범위한 범주로 나눌 수 있다. 트래픽 분류에 대한 고전적인 접근 방식은 IANA(Internet Assigned Numbers Authority)에 등록된 포트 번호를 응용 프로그램에 단순히 연결한다. 그러나 이제는 더 이상 유효한 방법이 아니다. 이처럼 포트 번호에만 의존하는 것은 효과가 없는 것으로 나타났다. 주로 동적 포트 협상, 터널링 및 잘 알려진 응용 프로그램에 할당된 포트 번호의 오용으로 인해 트래픽을 난독화하고 방화벽을 피할 수 있기 때문이다. 그럼에도 불구하고 다양한 트래픽 분류기는 성능을 개선하기 위해 다른 기술과 함께 포트 번호를 활용한다.

페이로드 기반 트래픽 분류는 포트 기반 트래픽 분류의 대안이다. 그러나 페이로드를 통해 알려진 애플리케이션 서명(signature)을 검색하기 때문에 더 높은 계산 및 저장 비용이 발생한다. 또한, 계속해서 증가하는 응용 프로그램과 그 역학에 따라 서명을 수동으로 유지 관리하고 적용하는 것은 번거롭다. 또한, 보안 및 개인 정보 보호 문제가 증가함에 따라 페이로드가 종종 암호화되고 개인정보보호법으로 인해 액세스가 금지된다. 따라서 페이로드를 사용하여 애플리케이션 클래스에 대한 서명을 추론하는 것이 간단한다.

호스트 동작 기반 트래픽 분류 기술은 네트워크에 있는 호스트의 고유한 동작 특성을 활용하여 관심 있는 클래스를 예측한다. 관찰 지점을 네트워크 에지로 이동하고 호스트 간의 트래픽을 검사하여 등록되지 않았거나 잘못 사용된 포트 번호 및 암호화된 패킷 페이로드의 한계를 극복한다 (예 : 연결되는 호스트 수, 전송 프로토콜, 관련 포트 수). 이러한 분류기는 애플리케이션이 서로 다른 통신 패턴을 생성한다는 개념에 의존한다. 예를 들어, P2P 호스트는 각 피어에 대해 다른 포트 번호를 사용하여 여러 다른 피어에 연결할 수 있다. 그러나 웹 서버는 동일

한 포트에서 다른 클라이언트에 의해 접속될 수 있다.

ML 기술	데이터셋	특징	클래스
지도 NB, AdaBoost, MaxEnt	proprietary	한 방향 플로우의 처음 n 바이트에 대한 이산 바이트 인코딩	FTP, SMTP, POP3, IMAP, HTTPS, HTTP, SSH
비지도 HCA	proprietary	한 방향 플로우의 처음 n 바이트에 대한 이산 바이트 인코딩	FTP, SMTP, HTTP, HTTPS, DNS, NTP, NetBIOS, SrvLoc
지도 SVM	Tstat, NAPA-WINE, proprietary	각 패킷의 처음 n 바이트의 통계적 특성	eMule, BitTorrent, RTP, RTCP, DNS, P2P-TV, Skype, Background
지도 SVM	proprietary	서비스 근접성, 활동 프로파일, 세션 기간, 주기성	Mail, Non-Mail
지도 SVM	proprietary	ΔT 동안 피어 사이에 교환된 패킷 수	PPLive, TVAnts, SopCast, Joost

표 4 페이로드 및 호스트 동작 기반 트래픽 분류 연구 동향

페이로드 기반 및 호스트 동작 기반 트래픽 분류기와 달리 플로우 특징 기반 분류기는 다른 관점을 갖는다. 한 걸음 물러나서 한 쌍의 완전한 플로우로 구성된 통신 세션을 고려한다. 완전한 플로우는 특정 애플리케이션 프로토콜을 사용하여 IP 주소에 있는 포트와 다른 IP 주소에 있는 다른 포트 간에 네트워크상의 연속 패킷을 단방향으로 교환하는 것이다. 5-tuple인 <srcIP, destIP, srcPort, destPort, protocol>로 식별된다. 예를 들어, 온라인 게임 세션의 전체 플로우는 소스에서 대상 d (예 : 호스트에서 게임 서버로)로 전송된 모든 순차적 패킷으로 구성된다. 따라서 전체 플로우에는 세션 설정, 데이터 교환 및 세션 해체와 관련된 모든 패킷이 포함된다. 하위 플로우는 전체 플로우의 하위 집합이며 진행 중인 세션에서 일정 기간 수집할 수 있다. 특징은 패킷 길이, 패킷 도착 간 시간, 플로우 기간 및 플로우의 패킷 수와 같은 플로우의 고유한 특성을 나타내는 속성이다. 플로우 특징 기반 기술은 플로우 특성을 구분자로 사용하여 플로우를 관심 있는 클래스에 매핑한다.

본질적으로 플로우 특징 기반 트래픽 분류는 다양한 애플리케이션에서 생성된 트래픽 풋 프린트의 다양성과 구별 가능한 특성을 활용한다. 등록되지 않은 포트 번호, 암호화된 패킷 페이로드, 라우팅 비대칭, 높은 저장 및 계산 오버헤드와 같은

다른 기술의 수많은 한계를 극복할 수 있는 잠재력이 있다. 그러나 플로우 특징 기반 분류기가 페이로드 기반 분류기의 정확도를 달성할 수 있는지 평가해야 한다.

ML 기술	데이터셋	특징	클래스
지도 *k*-NN	Proprietary	패킷 레벨 및 플로우 레벨 특징	Telnet, FTP-data, Kazaa, RealMedia Streaming, DNS, HTTPS
지도 NBKE	Proprietary	기저 및 유도 패킷 레벨 특징	BULK, WWW, Mail, 서비스, DB, P2P, Attack, 멀티미디어
지도 NBKE	Proprietary	기저 및 유도 패킷 레벨 특징	WWW, email, bulk, attack, P2P, multimedia, service, database, interaction, games
지도 REPTree, REPTree-Bagging	NLANR	패킷 레벨, 플로우 레벨, 연결 레벨 특징	WWW, Telnet, Messenger, FTP, P2P, Multimedia, SMTP, POP, IMAP, DNS, Services
지도 BoF-NB	WIDE, Proprietary	단방향 플로우의 패킷 레벨 및 플로우 레벨 특징	BT, DNS, FTP, HTTP, IMAP, MSN, POP3, SMTP, SSH, SSL, XMPP
지도 RF, 비지도 *k*-Means (BoF-based, RTC)	KEIO, WIDE, Proprietary	단방향 플로우의 패킷 레벨 및 플로우 레벨 특징	FTP, HTTP, IMAP, POP3, RAZOR, SSH, SSL, Unknown/Zero-day(BT, DNS, SMTP)
지도 BNN	Proprietary	패킷 레벨 및 플로우 레벨 특징	ATTACK, BULK, DB, MAIL, P2P, SERVICE, WWW
지도 PNN	Proprietary	패킷 레벨 및 플로우 레벨 특징	P2P, WEB, 기타
지도 SVM	LBNL, CAIDA, Proprietary	패킷 페이로드 크기	HTTP, SMTP, POP3, HTTPS, IMAPS, BitTorrent, FTP, MSN, eDonkey, SSL, SMB, Kazaa, Gnutella, NNTP, DNS, LDAP, SSH
지도 FT-SVM	Proprietary	12~248 특징의 부분집합	bulk, interactive, WWW, mail, 서비스, P2P, Attack, Game, Multimedia, 기타
지도 multi-class SVM, unbalanced binary SVM	Proprietary	플로우 레벨 및 연결 레벨 특징	BitTorrent, eDonkey, Kazaa, pplive

표 5 지도 플로우 특징 기반 트래픽 분류 연구 동향

ML 기술	데이터셋	특징	클래스
비지도 *k*-Means	Proprietary	패킷 레벨 및 플로우 레벨 특징	WWW, mail, P2P, ftp (control, pasv, data), attack, DB, 서비스, interactive, multimedia, games
비지도 AutoClass	NLANR	패킷 레벨 및 플로우 레벨 특징	AOL Messenger, Napster, Half-Life, FTP, Telnet, SMTP, DNS, HTTP
비지도 AutoClass	U. Auckland	패킷 레벨 및 플로우 레벨 특징	HTTP, SMTP, DNS, SOCKS, IRC, FTP (control, data), POP3, LIMEWIRE, FTP
비지도 DBSCAN	U. Auckland, proprietary(U. Calgary)	패킷 레벨 및 플로우 레벨 특징	HTTP, P2P, SMTP, IMAP, POP3, MSSQL, 기타
비지도 *k*-Means	Proprietary	한 방향 플로우의 패킷 레벨 및 플로우 레벨 특징	Web, email, DB, P2P, 기타, chat, FTP, streaming

표 6 비지도 플로우 특징 기반 트래픽 분류 연구 동향

ML 기술	데이터셋	특징	클래스
비지도 k-Means	proprietary	패킷 크기 및 한 플로우에서 처음 P 패킷의 방향	eDonkey, FTP, HTTP, Kazaa, NNTP, POP3, SMTP, SSH, HTTPS, POP3S
지도 J48 DT, k-NN, Random Tree, RIPPER, MLP, NB	proprietary	처음 N 패킷의 페이로드 크기 통계 및 인터패킷 시간 통계, 양방향 플로우 지속시간/크기, 트랜스포트 프로토콜	BitTorrent, SMTP, Skype2Skype, POP, HTTP, SOULSEEK, NBNS, QQ, DNS,SSL RTP, eDonkey
지도 NB, C4.5 DT	proprietary	인터패킷 도착 시각 통계, 인터패킷 길이 변화 통계, N 연속 패킷의 IP 패킷 길이 통계	Enemy Territory (online game), VoIP, Other
Semi-supervised k-Means	proprietary	패킷의 수, 평균 패킷 크기, 전체 바이트 수, 전체 헤더 바이트 수, 전체 페이로드 바이트 수	P2P, HTTP, CHAT, EMAIL, FTP, STREAMING, OTHER
지도 C4.5 DT, C4.5 DT with AdaBoost, NBKE	proprietary	처음 N 패킷의 248개 특징 중 12개	WEB, MAIL, BULK, Attack, P2P, DB, Service, Interactive
지도 AdaBoost	proprietary	lowsrcport, highsrcport, duration, 평균 패킷 크기, 평균 패킷율, toscount, tcpflags, dstinnet, lowdstport, highdstport, 패킷 바이트, tos, numtosbytes, srcinnet	Business, chat, DNS, FileSharing, FTP, Games, Mail, Multimedia, NetNews, SecurityThreat, VoIP, Web
지도 NB, Pearson's χ^2 test	proprietary	메시지 크기, 평균 패킷 간 갭(gap)	Skype
지도 AdaBoost, SVM, NB, RIPPER, C4.5 DT	AMP, MAWI, DARPA99, proprietary	패킷 크기, 패킷 간 도착 시각, 패킷의 수, 바이트 수, 플로우 지속시간, 프로토콜	SSH, Skype
지도 C4.5 DT, RF	synthetic trace	암호화된 페이로드의 통계적 특성	Service Provider (# of services): Uni-lorraine.fr(15), Google.com(29), akamihd.net(6), Googlevideo.com(1), Twitter.com(3), Youtube.com(1), Facebook.com(4), Yahoo.com(19), Cloudfront.com(1)

표 7 Early, 서브플로우 기반 및 암호화된 플로우 기반 트래픽 분류 연구 동향

ML 기술	데이터셋	특징	클래스
지도 k-NN, Linear-SVM, Radial-SVM, DT, RF, Extended Tree, AdaBoost, Gradient-AdaBoost, NB, MLP	KDD	Protocol, network service, source bytes, destination bytes, login status, error rate, connection counts, connection percentages (different services among the same host, different hosts among the same service)	공격 유형
지도 RF, SGBoost, XGBoost	proprietary	Packet size (1 to N packets), packet timestamp (1 to N packets), inter-arrival time (N packets), source/destination MAC, source/destination IP, source/destination port, flow duration, packet count byte count	BitTorrent, Dropbox, Facebook, Web Browsing (HTTP), LinkedIn, Skype, Vimeo, YouTube
준지도 Laplacian-SVM	proprietary	Entropy of packet length, average packet length (source to destination and vice versa), source port, destination port, packets to respond from source to destination, minimum length of packets from destination to source, packet inactivity degree from source to destination, median of packet length from source to destination for the first N packets	Voice/video conference, streaming, bulk data transfer, interactive

표 8 NFV/SDN 기반 트래픽 분류 연구 동향

3.2.3 트래픽 라우팅

네트워크 트래픽 라우팅은 네트워킹의 기본이며 패킷 전송 경로를 선택해야 한다. 선택 기준은 다양하며 주로 비용 최소화, 링크 활용 극대화 및 QoS 프로비저닝과 같은 운영 정책 및 목표에 따라 다르다. 트래픽 라우팅에는 복잡하고 동적인 네트워크 토폴로지에 대처하고 스케일링하는 능력, 선택한 경로와 인지된 QoS 간의 상관관계를 학습하는 능력, 라우팅 결정의 결과를 예측하는 능력 등 ML 모델에

대한 까다로운 능력이 필요하다. 기존 문헌을 검토해보면 트래픽 라우팅을 지배한 ML 기술은 강화학습이다.

기술(선택)	응용(네트워크)	데이터셋	특징	Action set
부분적 탈중앙화 LSPI (ε-greedy)	유니캐스트 라우팅(WSN)	시뮬레이션 ·센서: 400개 ·데이터 소스: 20개 ·싱크: 1개	State: N_i Reward: function of · node load · residual energy · hop cost to sink · link reliability	Next-hop nodes to destination
Q-learning (variant of ε-greedy)	멀티캐스팅 라우팅 (WSN)	Omnet++ with 50 random topologies ·50 nodes ·5 sources ·45 sinks	State: (N_i^k, D_k) Reward: function of hop cost	$a_1, \cdots, a_m$ $a_k = (N_j^k, D_k)$ N_j^k = next hop along the path to sink D_k
Variant of Q-learning (ε-greedy)	Localization-aware routing to achieve a trade-off between packet delivery rate, ETX, and network lifetime (WSN)	시뮬레이션 ·50 different topologies ·100 nodes	State: N_i Reward: function of · distance(N_i, N_j) · distance(N_j, d) · energy at N_j · ETX · N_j's neighbors for any neighbor N_j and destination	Next-hop nodes to destination
DRQ-learning (greedy)	Spectrum-aware routing (CRN)	OMNET++ sim. ·stationary multi-hop CRN ·10 nodes, 2 PUs	State: N_i Reward: # available channels between current node and next-hop node	Next-hop nodes to destination
모델 기반 Q-learning (greedy)	Distributed energy-efficient routing (underwater WSN)	시뮬레이션 (ns-2) ·250 sensors in 5003 m^3 space ·100m tx range ·fixed source/sink ·1m/s max speed for intermediate nodes	State: N_i Reward: function of the residual energy of the node receiving the packet and the energy distribution among its neighbor nodes.	Next-hop nodes to destination ∪ packet withdrawal
n−step TD (greedy)	Delay-sensitive application routing (multi-hop wireless ad hoc networks)	시뮬레이션 ·2 users transmitting video sequences to the same destination ·3~4-hops wireless network	State: current channel states and queue sizes at the nodes in each hop Reward: goodput at destination	Next-hop nodes to destination
Q-learning with adaptive learning rate (ε−greedy)	Opportunistic routing (multi-hop wireless ad hoc networks)	Simulations on QualNet with 36 randomly placed wireless nodes in a 150m×150m	State: N_i Reward: · fixed negative tx cost if receiver is not the dst · fixed positive reward if receiver is the dst · 0 if packet is withdrawn	Next-hop nodes to destination U packet withdrawal
Centralized SARS (ε−greedy)	QoS-aware adaptive routing (SDN)	Sprint GIP network trace-driven sim. · 25 switches, 53 links	State: N_i Reward: function of delay, loss, throughput	Next-hop nodes to destination

표 9 RL(Reinforcement Learning) 기반 탈 중앙화(decentralized), 부분적 탈 중앙화(partially decentralized) 및 중앙집중식(centralized) 라우팅 모델 연구 동향

3.2.4 혼잡 제어

혼잡 제어는 네트워크 운영의 기본이며 네트워크로 들어오는 패킷 수를 조절하는 역할을 한다. 네트워크 안정성, 자원 활용의 공정성 및 허용 가능한 패킷 손실 비율을 보장한다. 다양한 네트워크 아키텍처는 자체 혼잡 제어 메커니즘 세트를 배포한다. 가장 잘 알려진 혼잡 제어 메커니즘은 TCP에서 구현된 것이다. IP와 함께 TCP가 현재 인터넷의 기반을 구성하기 때문이다. TCP 혼잡 제어 메커니즘은 혼잡이 감지될 때 패킷 전송 속도를 제한하기 위해 네트워크의 최종 시스템에서 작동한다. 잘 알려진 또 다른 혼잡 제어 메커니즘은 TCP를 보완하기 위해 네트워크의 중간 노드 (예 : 스위치 및 라우터) 내에서 작동하는 대기열 관리이다. 인터넷 및 DTN (Delay Tolerant Networks) 및 NDN (Named Data Networking)과 같은 진화 네트워크 아키텍처를 위한 혼잡 제어 메커니즘이 몇 가지 개선되었다. 이러한 노력에도 불구하고 패킷 손실 분류, 대기열 관리, CWND (Congestion Window) 업데이트 및 혼잡 추론과 같은 영역에는 다양한 단점이 있다.

ML 기술	네트워크	데이터셋	특징	분류
비지도: EM for HMM	Hybrid wired and wireless	-Synthetic data: · ns-2 sim. · 4-linear topo. -Data distribution: · Training=10k	Loss pair RTT	· 혼잡 손실 · 무선 손실
비지도: EM for HMM	Hybrid wired and wireless	Synthetic data: ·ns-2 sim. ·Topology: - 4-linear - Dumbbell	· Loss pair delay · Loss probabilities: - Congestion - Wireless	· 혼잡 손실 · 무선 손실
지도: ·Boosting DT ·DT ·RF ·Bagging DT ·Extra-trees ·MLP-NN ·*k*-NN	Hybrid wired and wireless	ㅇSynthetic data: · Sim. in: - ns-2 - BRITE · >1k random topologies ㅇData distribution: · Training = 25k · Testing = 10k	40 features applying avg, stdev, min, and max on parameters: · One-way delay · IAT And on packets: · 3 following loss · 1 before loss · 1/2 before RTT	· 혼잡 손실 · 무선 손실
지도: Bayesian	Wired	Real data: · PMA project · BU Web server	Loss pair RTT	· 혼잡 손실 · 재정렬
비지도: ·EM for HMM ·EM-clustering	Optical	Synthetic data: · ns-2 sim. · NSFNET topo. Data distribution: · Training = 25k · Testing = 15k	Number of bursts between failures	· 혼잡 손실 · 경쟁 손실

표 10 네트워크의 엔드 시스템에서 오프라인 훈련을 이용한 패킷 손실 분류 연구 동향

Ref.	ML 기술	Multiple Bottleneck	Synthetic data from ns-2 sim.	특징	출력 (action set for RL)
PAQM	지도 OLS	√	Topology: ·6-linear ·임의의 dumbbell Time = 50s	Traffic volume (bytes)	TSF: · Traffic volume
APACE	지도 OLS	√	Topology: ·Dumbbell (1-sink) ·6-linear Time = 40s	Queue length	TSF: · Queue length
α_SNFAQM	지도 MLP-NN	-	Topology: ·Dumbbell (1-sink) Time = 300s	· Traffic volume · Predicted traffic volume	TSF: · Traffic volume
NN-RED	지도 SLP-NN	-	Topology: Dumbbell Time = 900s	Queue length	TSF: · Queue length
DEEP BLUE	강화: ·Q-learning ·ε-greedy	-	Topology: Dumbbell Time = 50s OPNET instead of ns-2	States: · Queue length · Packet drop prob. Reward: · Throughput · Queuing delay	Decision making: · Increment of the packet drop probability (finite: 6 actions)
Neuron	강화: PIDNN	√	Topology: Dumbbell Time = 100s	Queue length error	Decision making: · Increment of the packet drop probability (continuous)
AN-AQM	강화: PIDNN	√	Topology: · Dumbbell · 6-linear Time = 100s	· Queue length error · Sending rate error	Decision making: · Increment of the packet drop probability (continuous)
FAPIDNN	강화: PIDNN	√	Topology: Dumbbell Time = 60s	Queue length error	Decision making: · Increment of the packet drop probability (continuous)
NRL	강화: SLP-NN	√	Topology: Dumbbell Time = 100s	· Queue length error · Sending rate error	Decision making: · Increment of the packet drop probability (continuous)

표 11 유선 네트워크의 중간 노드에서 온라인 트레이닝하는 AQM 기법 연구 동향

Ref.	ML 기술	네트워크	Synthetic data set	특징	Action set (selection)
TCP-FALA	FALA	WANET	GloMoSim · topology · random · dumbbel	States and reward: · IAT of ACKs	5 actions
Learning-TCP	CALA	WANET	Simulation: · ns2, GloMoSim · Topology: - Chain - Random node - Grid Experimental: · Linux-based · Chain topology	States and reward: · IAT of ACKs	Continuous: · Normal action probability distribution (stochastic)
TCP-GVegas	Q-Learning	WANET	ns-2 sim: · Topology: - Chain - Random	States: · CWND, RTTz · Throughput Reward: · Throughput	Continuous: · Range based on RTT, throughput, and a span factor (ε-greedy)
FK-TCPLearning	FKQL	IoT	ns-3 sim: · Dumbbell topology: - Single source/sink - Double source/sink	States: · IAT of ACKs · IAT of packets sent · RTT, SSThresh Reward: · Throughput · RTT	5 actions (ε-greedy)
UL-TCP	CALA	Wireless: ·Single-hop: Satellite, Cellular, WLAN ·Multi-hop: WANET	ns-2 sim: · Single-hop dumbbell · Multi-hop topo: - Chain - Random - Grid	States and reward: · RTT · Throughput · RTO CWND	Continuous: · Normal action probability distribution (stochastic)
Remy	Own (offline traning)	· Wired · Cellular	ns-2 sim: · Wired topology: - Dumbbell - Datacenter · Cellular topology	States: · IAT of ACKs · IAT of packets sent · RTT Reward: · Throughput · Delay	Continuous with 3-dimensions: · CWND multiple · CWND increment · Time between successive sends (ε-greedy)
PCC	Own	· Wired · Satellite	Experimental: · GENI · Emulab · PlanetLab	States: · Sending rate Reward: · Throughput · Delay · Loss rate	· 2 actions of the increment for updating sending rate (not CWND) (gradient ascent)

표 12 네트워크의 엔드 시스템에서 온라인 트레이닝을 사용하여 CWND 갱신을 위한 증가량에 대한 의사 결정에 관한 연구 동향

ML 기술	네트워크(위치)	데이터셋	특징	출력
지도: · MLP-NN · MART · Bagging DT · Extra-trees (offline)	유선 (엔드 시스템)	Synthetic data: · ns-2 simulation · > 1k random topo. Data distribution: · Training = 18k · Testing = 7.6k	· Packet size · RTT: avg, min, max, stdev · Sesion loss rate · Initial timeout · Packets ACK at once · Session duration · TLR	예측: · throughput
지도: · SVR (offline)	다중경로 유선 (엔드시스템)	Synthetic data: · Laboratory testbed -Dumbbell 다중경로 topo. · RON testbed	· Queuing delay · Packet loss · Throughput	예측: · throughput
지도: · BN (offline)	WLAN (AP)	Synthetic data: · ns-3 simulation · Star topology Data distribution: · Training = 40k · Testing = 10k	· MAC-TX/RX · MAC contention window · CWND, CWND status · RTT · Trhoughput	예측: · throughput
지도: · BN (offline)	WANET (엔드시스템)	Synthetic data: · ns-3 simulation · Topology: - (not mentioned)	· MAC-TX/RX · Slots before TX · Queue TX packets · Missing entries in IP table	분류: · Static · Mobile
지도: · WMA (online)	WANET ·유선 ·하이브리드 유무선 (엔드시스템)	Synthetic data: · QualNet simulation · Topology: - Random WANET - Dumbbell wired Real data: · File transfer · Wired and WLAN	RTT	예측 : RTT
지도: WMA (online)	하이브리드 유무선 (엔드시스템)	real data	RTT	예측: RTT
지도: · TLFN - PSO - GA (online)	NDN (제어기 노드)	Synthetic data: · ns-2 simulation · Topology: - DFN - SWITCH Data distribution: · Training = 70% · Validation = 15% · Testing = 15%	PIT entires rate	예측: PIT entries rate
강화: · Q-learning - Boltzmann - WoLF (online)	DTN (노드)	Synthetic data: · ONE simulation: · Random topology	States: · Input rate · Output rate · Buffer space Reward: · State transition	States: · Input rate · Output rate · Buffer space Reward: · 상태 천이

표 13 서로 다른 네트워크 파라미터의 추정으로부터 혼잡 추론에 관한 연구 동향

3.2.5 자원 관리

네트워킹의 자원 관리에는 CPU, 메모리, 디스크, 스위치, 라우터, 대역폭, AP, 무선 채널 및 해당 주파수를 포함한 네트워크의 중요한 자원을 제어하는 것이 수반된다. 이들은 서비스를 제공하기 위해 집합적으로 또는 독립적으로 활용된다. 단순하게 네트워크 서비스 제공 업체는 서비스에 대한 예상 수요를 맞추는 고정된 양의 자원을 프로비저닝 할 수 있다. 그러나 수요를 예측하는 것은 사소한 일이 아니지만, 과도하거나 과소평가하면 활용률이 떨어지고 수익에 있어 손실을 낳을 수도 있다. 따라서 자원 관리의 근본적인 과제는 수요를 예측하고 자원을 동적으로 프로비저닝 및 재 프로비저닝 하는 것이다. 따라서 네트워크는 서비스 수요의 변화에 대해 탄력적이다. 클라우드 데이터센터의 부하 예측 및 자원 관리를 위한 ML의 광범위한 적용에도 불구하고, 셀룰러 네트워크, 무선 네트워크 및 애드혹 네트워크를 포함한 다양한 네트워크에서 여전히 다양한 문제가 발생하고 있다. 자원 관리에는 여러 가지 문제가 있지만, 여기에서는 수락 제어와 자원 할당이라는 두 가지 범주만 살펴본다.

수락 제어는 수요 예측이 필요 없는 자원 관리에 대한 간접적인 접근 방식이다. 수락 제어의 목적은 네트워크의 자원을 모니터링하고 관리하여 자원 활용을 최적화하는 것이다. 예를 들어, 컴퓨팅 및 네트워크 자원에 대한 새로운 요청은 VoIP 통화 또는 연결 설정을 위해 시작된다. 이 경우 수락 제어는 사용 가능한 네트워크 자원, 새 요청의 QoS 요구사항 및 네트워크의 자원을 사용하는 기존 서비스에 관한 결과를 기반으로 새 수신 요청을 승인할지 거부할지를 지정한다. 새로운 요청을 수락하면 네트워크 서비스 공급자에게 수익이 발생한다. 그러나 자원 부족으로 기존 서비스의 QoS를 저하하고 결과적으로 SLA를 위반하여 벌금 및 수익 손실을 초래할 수 있다. 따라서 새로운 요청을 받아들이는 것과 QoS 유지 또는 충족 사이에 trade-off가 있어야 한다. 수락 제어는 이러한 문제를 해결하고 SLA를 위반하지 않고 네트워크에서 수락하고 처리하는 요청 수를 최대화하는 것을 목표로 한다.

반대로 자원 할당은 수익 또는 자원 활용과 같은 장기 목표를 극대화하기 위해 자원을 적극적으로 관리하는 의사 결정 문제이다. 자원 할당의 근본적인 과제는 예측 불가능성에 직면하여 장기적인 이익을 위해 자원을 조정하는 것이다. 자원 할당에 대한 일반적인 모델 기반 접근 방식은 네트워크에서 자원 요청의 속도와 볼륨을 따라잡는데 부족했다. 그러나 자원 할당은 다양한 방법으로 자원 프로비저닝을 학습하고 관리할 수 있는 ML의 장점을 강조하기 위한 예시이다.

ML 기술	네트워크	데이터셋	특징	출력
지도 MLP-NN	무선망	ns-Miracle을 이용하여 발생한 시뮬레이션 데이터	· SNR · 수신 프레임 · 오류 프레임 · Idle time	· 처리율 · 지연 · 신뢰도
지도 MLP-NN	무선 LAN	Synthetic data generated using testbed	· SNR · 실패 확률 · business ratio · 평균 비콘 지연 · 탐지된 단말의 수	· AP의 처리율
RNN with GD, AIWPSO, and DE	셀룰러	Synthetically generated using a SEAMCAT LTE simulator	· SNR · 셀간 간섭 · 변조/코딩 기법 · 전송 출력	처리율
지도: 선형분류기 비지도: RNN	무선망	38 video clips taken from CIF	비디오 프레임 크기	평균 SSIM 지수로 나타낸 각 비디오의 품질 수준
강화: Q-learning	VNs	Simulation on ns-3 and real Internet traffic traces	States: substrate 노드와 링크에서 할당되었으나 사용하지 않는 자원의 %	동작: 할당된 자원의 퍼센티지를 증가 또는 감소
지도 FNN	VNF 체인	VoIP traffic traces	· 각 VNFC 자원 요구사항이 이웃 VNFC에 의존하는 정도 · 로컬 VNFC 자원 활용도 이력	각 VNFC의 자원 요구사항
지도: MDP, BN	VNF 체인	Simulation data generated using WorkflowSim	자원 이용 이력	미래 자원 의존도

표 14 ML 기반 자원 할당에 관한 연구 동향

ML 기술	네트워크	데이터셋	특징	출력
지도 NN	ATM	simulation	· 링크 용량 · 관찰된 호 발생률	호 손실률
지도 MLP-NN	ATM	simulation	· Congestion-status · Cell-loss probability · Peak bitrate · Average bitrate · Mean peak-rate duration	수락 또는 거부
지도 RandNN	무선	videos by streaming app	Codec, bandwidth, loss, delay, and jitter	MOS
지도 MLP-NN	WLAN	ns-3, testbed	링크 부하 및 프레임 손실	서비스 품질
지도 MLP-NN	CDMA	simulation	· 네트워크 환경 · 사용자 행태 · 호 클래스 · 액션	GoS
지도 MLP-NN	LTE	ns-3	· Application throughput · Average packet error rate · Average size of packet data unit	QoS fulfillment ratio
지도 : · MLP · Prob. RBFNN · LVQ-NN · HNN · SVM network	Ad hoc networks	Pamvotis	· 네트워크 처리율 · 패킷 발생률	평균 패킷 지연
비지도 HNN	무선	simulation	사용가능한 QoS 수준	QoS assignment matrix for each connection
지도 RNN	VN	simulation	Different graph features	VN의 수락 또는 거부
지도: NN, BN	LTE	ns-3	Channel quality indicator	R-factor
지도 BN	WLAN	ns-3	Link Layer conditions	음성 전화 품질
강화 Q-learning	NGN	OMNET	States · Environment state based on number of active connections of each traffic class	Action: 수락 또는 거부 (ε- greedy)
강화 Q-learning	LTE femtocell	simulation	States · Queue length of handoff and new calls	Action · Maintain,degrade, or upgrade proportion levels
강화 Q-learning	Multimedia networks	simulation	States · The number ongoing calls of each class · Call arrival or termination event · QoS and capacity constraints	Action: 수락, 거절, 무대응
강화: TD	Integrated service networks	simulation	States · The number active calls of each class · Routing path of each active call	경로로 수락 또는 거부

표 15 ML 기반 수락 제어(Admission Control)에 관한 연구 동향

3.2.6 결함 관리(Fault Management)

결함 관리에는 네트워크의 비정상 상태를 감지, 격리 및 수정하는 작업이 포함된다. 네트워크 운영자와 관리자는 전체 네트워크, 해당 장치 및 네트워크에서 실행되는 모든 응용 프로그램에 대한 철저한 지식을 가지고 있어야 한다. 이것은 비현실적인 기대이다. 또한, 가상화 및 소프트웨어화와 같은 최근 기술 발전으로 인해 오늘날의 네트워크는 크기, 복잡성 및 매우 동적인 면에서 기념비적이다. 따라서 오늘날의 네트워크에서 장애 관리가 점점 더 어려워지고 있다.

단순한 결함 관리는 피동적이며 결함의 감지, 국소화 및 완화의 주기적인 프로세스로 인식될 수 있다. 첫째, 결함 감지는 다양한 네트워크 증상을 공동으로 연관지어 하나 이상의 네트워크 장애 또는 결함이 발생했는지 확인한다. 예를 들어, 스위치 용량 감소, 특정 애플리케이션의 패킷 생성 속도 증가, 스위치 비활성화 및 링크 비활성화로 인해 결함이 발생할 수 있다. 따라서 결함 관리의 다음 단계는 결함의 근본 원인을 파악하는 것이다. 이 경우 결함이 있는 네트워크 하드웨어 또는 소프트웨어 요소의 물리적 위치를 정확히 찾아내고 결함의 원인을 결정해야 한다. 마지막으로 결함 완화는 네트워크 동작을 수리하거나 수정하는 것을 목표로 한다. 반대로, 결함 예측은 사전예방적이며 성능 저하를 최소화하기 위해 결함을 예측하고 완화 절차를 시작하여 향후 결함 또는 장애를 방지하는 것을 목표로 한다. ML 기반 기술은 이러한 문제를 해결하고 결함 예측, 감지, 근본 원인의 국소화 및 결함 완화의 영역에서 인지적 결함 관리를 촉진하기 위해 제안되었다.

ML 기술	네트워크	데이터셋	특징	출력
지도 BN	캠퍼스	라우터에서 수집한 데이터	인터페이스, IP, 및 UDP 그룹에 대한 MIB 변수	네트워크 건강 예측
지도 BN	셀룰러	오류를 삽입한 시뮬레이션	전력, 멀티플렉서, 셀, 전송	결함 여부
지도 NN(MLP)	무선망	이산 시간 이벤트 시뮬레이션에서 생성	MTTF, MTTR, 시간 프로파일, 런 타임	네트워크의 신뢰성 · 생존성 · 가용성 · 고장난 부품 · 보고 가능한 중단
지도: · DT (J4.8) · Rule learners (JRip) · SVM · BN · Ensemble	WSN	센서 네트워크 테스트베드에서 생성	RSSI, 송수신 버퍼 크기, 채널 부하 평가, forward and backward	링크 품질 추정
Manifold learning: SHLLE	분산 시스템	파일 전송 응용을 갖는 분산 환경의 테스트베드에서 생성	시스템 성능, 인터페이스 그룹, IP 그룹, TCP/UDP 그룹	네트워크, CPU 및 메모리 고장의 예측
· 선형 회귀 · M5P · REP-Tree · LASSO · SVM · Least-Square SVM	멀티티어 e-commerce 웹 응용	가상 구조의 테스트베드에서 생성	상이한 시스템 성능	RTTF
지도: DES, SVM	optical	telco의 광 네트워크에서 수집된 실제 데이터	보드 데이터에 있는 표시기 : · 입력 광 전력 · 레이저 바이어스 전류 · 레이저 온도 오프셋 · 출력 광 전력 · 환경 온도 · 사용할 수 없는 시간	장비 고장 예측
비지도: DNN with Autoencoders	셀룰러	미국의 한 이통사에서 수집한 한달 동안의 결함 데이터	결함 발생 및 결함 발생 간격에 대한 이력 데이터	결함 발생 시간 간격 예측

표 16 ML 기반 결함(fault) 예측에 관한 연구 동향

ML 기술	네트워크	데이터셋	특징	출력
통계적 학습	셀룰러	실제 셀룰러망의 데이터	모바일 사용자 호 부하 프로파일	기지국, 섹터, 캐리어, 채널 수준에서 결함 감지
NN의 조합	셀룰러	OPNET Sim.	각 결함 시나리오에 대해 · 패킷 차단 · 큐 크기 · 패킷 처리량 · 서브넷을 연결하는 링크 활용도 · 패킷 종단 간 지연	결함 시나리오 중 하나 감지 · 줄어든 스위치 용량 · 특정 응용의 늘어난 패킷 발생 · 비활성화된 스위치 · 비활성화된 링크
지도: k-Means, FCM, EM	학교 캠퍼스의 IP 망	트래픽이 많고 적은 시나리오가 있는 네트워크에서 획득	SNMP를 통해 수집된 12개의 범주의 IF 변수	결함 클래스 · 정상 트래픽 · 링크 장애 트래픽 · 서버 다운 · 브로드캐스트 스톰 · 프로토콜 오류
지도: RNN	WSN	센서망 시뮬레이션에서 수집	센서 노드의 이전 출력 이웃 센서 노드의 현재 및 이전 출력 샘플	센서 노드 출력의 근사값
비지도 변화 감지법	LAN	원격 모니터링 에이전트를 사용하여 실제망에서 수집	baseline 랜덤 변수	이상이 발생하는 즉시 알람
지도: k-Means, FCM, SOM	광대역 서비스 제공자 망	5 서비스 영역에서 백만개 NFL 데이터 포인트	결함 발생일, 시간, 지리적 지역, 결함 원인, 해결 시간	긴 결함 해결 시간과 관련된 시공간 패턴 식별

표 17 ML 기반 결함 탐지(fault detection)에 관한 연구 동향

ML 기술	네트워크	데이터셋	특징	출력
DT(C4.5)	네트워크 시스템	eBay 로그의 스냅샷	요청의 완전한 트레이스 · 요청 형태/명 · 풀(pool), 호스트, 버전 · 각 요청의 현황	상이한 결함 요소
BN	광 네트워크	종합적으로 발생된 시계열	전송 품질 (QoT) 매개 변수 · 수신 전력 · Pre-forward 오류 정정 비트 오류율 (pre-FEC BER)	두 가지 결함 시나리오 중 하나 감지 · 빡빡한 필터링 · 채널간 간섭
BN, EMD	셀룰러 네트워크	UMTS 망의 시뮬레이션과 실제 망에서 종합적으로 생성	· 결함의 원인 · 경보 및 KPI 같은 증상	결함 원인 식별
지도: DT(ID3)	3-tier 기업 응용	소규모 테스트베드 플랫폼에서 생성	정상 또는 비정상으로 분류되는 경로들	장애와 관련있는 HW 및 SW 구성 요소
비지도: discrete state-space particle filtering	IP 네트워크	Discrete event simulator	· 활성 네트워크 측정 · 확률 추론 · 변화 감지	결함있는 구성요소의 위치를 나타내는 pmf
비지도: WTA, FSCL, SOM, NGA	셀룰러 네트워크	simulation	네트워크의 정상적인 기능을 나타내는 상태 벡터	비정상을 일으키는 상태 벡터

표 18 ML 기반 결함 국소화(fault localization)에 관한 연구 동향

3.2.7 QoS/QoE 관리

네트워크 성능이 사용자 경험에 미치는 영향에 대한 지식은 서비스의 성공, 저하 또는 실패를 결정하므로 매우 중요하다. 사용자 경험 평가는 많은 관심을 끌었다. 초기 작업에서는 사용자 경험과 네트워크 QoS 간에 차이가 없었다. 그런 다음 사용자 경험은 네트워크 매개 변수 (예 : 대역폭, 패킷 손실률, 지연, 지터) 및 멀티미디어 서비스의 비트 전송률과 같은 애플리케이션 매개 변수로 측정되었다. QoS 매개 변수를 모니터링하고 제어하는 것은 높은 서비스 품질을 제공하는 데 필수적이지만, 특히 서비스 제공 업체의 경우 사용자 관점에서 서비스 품질을 평가하는 것이 더 중요하다.

사용자 QoE 평가는 개인의 경험이 개인의 기대와 인식에 따라 달라지기 때문에 복잡하다. 둘 다 본질적으로 주관적이며 정량화하고 측정하기가 어렵다. QoE 평가 방법은 지난 10년 동안 주관적인 테스트에서 객관적인 품질 모델링을 통한 참여 측정에 이르기까지 다양한 단계를 거쳤다. 사용자에게 MOS (평균 의견 점수, Mean Opinion Score)로 평균화된 의견 점수를 평가하거나 할당하도록 요청하는 주관적 테스트가 지금까지 널리 사용되고 있다. 주관적 테스트는 간단하고 구현하기 쉬우며 MOS 메트릭은 계산하기 쉽다. 그러나 사용자가 서비스를 평가하고 객관적으로 평가하도록 강요할 수 없으므로 MOS 점수는 불공평하고 편향될 수 있으며 이상치의 영향을 받는다. 비디오 품질 메트릭 (VQM), 음성 품질 (PESQ) 메트릭의 지각 평가, 음성 및 비디오 서비스에 대한 E- 모델과 같은 객관적인 품질 모델이 서비스를 객관적으로 평가하기 위해 제안되었다. 인간에 의해 품질이 향상되고보다 “공정“하고 편파적이지 않은 MOS를 추론한다. PESQ 및 VQM과 같은 full-reference (FR) 품질 모델은 원래 신호를 수신된 신호와 비교하여 품질 왜곡을 계산한다. 정확하지만 계산에 큰 노력이 필요하다. 반대로 E- 모델과 같은 no-reference (NR) 모델은 원래 신호에 대한 참조 없이 왜곡된 신호의 품질을 평가하려고 한다. 계산하기에 더 효율적이지만 정확도가 떨어질 수 있다. 최근에는 서비스 시간 및 수익 가능성과 같은 측정 가능한 사용자 참여 지표가 데이터 기

반 QoE 분석에서 나타났다. 이러한 메트릭은 콘텐츠 제공 업체에 대한 사용자 품질 인식의 영향을 보다 직접 끌어내는 것으로 밝혀졌다.

통계 및 ML 기술은 QoE를 네트워크 및 애플리케이션 수준 QoS에 연결하고 후자가 전자에 미치는 영향을 이해하는데 유용한 것으로 밝혀졌다. 선형 및 비선형 회귀 (예 : 지수, 로그, 전력 회귀)를 사용하여 사용자의 QoE 관점에서 네트워크 및 애플리케이션 수준 QoS 매개 변수 (예 : 패킷 손실 비율, 지연, 처리량, 왕복 시간, 비디오 비트 레이트, 프레임 속도 등)의 개별적 및 집합적 영향을 정량화했다. 문헌에서는 단일 기능을 가진 단순 회귀 모델이 가장 우세하지만, 서로 다른 QoS 매개 변수의 집합적인 영향도 고려되었다.

ML 기술	응용	데이터셋	특징	출력
지도 HMM (offline)	비디오 스트리밍에 대한 QoE를 개선하기 위해 HAS 클라이언트에서 미드스트림 비트율 적응을 위한 처리량 예측	아래를 포함하는 2천만 세션으로 구성된 iQIYI dataset ·3백만 클라이언트 IP ·18 서버 IPs ·87 ISPs	처리량 표본	1~10주기 앞선 처리량
강화 Q-learning (online)	다양한 네트워크 조건에서 QoE를 최대화하기 위해 HAS 클라이언트에서 비디오 품질 조정	노르웨이 Telenor 3G/HSDPA 이동무선망 데이터셋의 TCP 스트리밍 세션에 기반한 ns-3 시뮬레이션	State: · client buffer filling level · client throughput level Reward: QoE as function of · targeted quality level · span between current and targeted video quality level · rebuffering level	7가지 가능한 비디오 품질 수준의 유한 작업 집합

표 19 HAS 및 DASH를 위한 ML 기반 QoS/QoE 예측 모델에 관한 연구 동향

ML 기술	응용 (접근법)	데이터셋	특징	출력
ANFIS	네트워크 및 응용 수준 QoS가 무선 모바일 네트워크상에서 MPEG4 비디오 스트리밍에 미치는 영향 (NR 회귀)	Evalvid와 ns-2 시뮬레이션 · MPEG4 비디오 소스 · 3 가지 비디오 유형 · 가변 네트워크 조건 · 모바일 비디오 스트리밍 클라이언트 · PSNR 생성 MOS	비디오 유형 · 응용 프로그램 관련 : 프레임율, 전송 비트율 · 네트워크 수준 : 링크 대역폭, 패킷 오류율	MOS
MLP-NN	QoE에 대한 QoS 및 비디오 특성의 영향 (FR / NR 회귀)	Evalvid와 ns-2 시뮬레이션 · 3 가지 비디오 유형 (약간, 부드럽게, 빠른 동작) · 565 데이터 포인트 · Evalvid 및 VQM 도구에서 생성된 MOS, PSNR, SSIM 및 VQM	지연, 지터, total/I/P/B 프레임 손실	모델 출력: MOS, PSNR, SSIM, VQM
DT, RF, NB, SVM, *k*-NN, and NN	QoE에 대한 QoS, 비디오 기능 및 뷰어 기능의 영향 (NR 분류)	QoS가 제어되는 에뮬레이트된 네트워크를 통해 스트리밍 비디오에서 수집되고, 시청자 패널에서 수집된 MOS	네트워크 수준: 지연, 지터, 패킷 손실 등 응용 관련: 해상도 비디오 유형: 동작 복잡도 시청자 관련: 성(性), 관심사 등	MOS
SVR, MLP-NN, DT, and GNB	VoIP 서비스에 대한 QoE 및 네트워크 QoS 메트릭의 모듈식 사용자 중심 상관관계 (NR 회귀)	OMNET ++로 생성된 다양한 네트워크 조건에서 VoIP 세션의 3개 데이터 세트 : 핸드 오버 중 (데이터 세트 1), UDP 트래픽이 많은 네트워크 (데이터 세트 2), TCP 트래픽이 많은 네트워크 (데이터 세트 3) 사용자 생성 MOS 및 프로그램 생성 PESQ 및 E-model QoE로 평가된 QoE	네트워크 관련: 지연, 지터, 패킷 손실 등	MOS
RF, BG, and DNN	비디오 스트리밍 서비스에 대한 QoE와 네트워크 및 애플리케이션 QoS 메트릭의 상관관계(NR 회귀)	다양한 비디오 및 네트워크 매개 변수로 인코딩 및 전송된 시청각 시퀀스에 대한 사용자 생성 MOS를 포함한 INRS 데이터 세트	네트워크 관련: 지연, 지터, 패킷 손실 등 응용 관련: 비디오 프레임율, 양자화 파라미터, 필터 등	MOS

표 20 지도 ML 기반 QoS/QoE 상관 모델에 관한 연구 동향

3.2.8 네트워크 보안

네트워크 보안은 네트워크의 가용성을 손상하거나 네트워크 액세스 가능한 자원의 무단 액세스 또는 오용을 초래할 수 있는 사이버 위협으로부터 네트워크를 보호하는 것이다. 기업은 지속해서 보안 위협에 처해 있으며, 이는 많은 손상 및 복구 비용이 들뿐만 아니라 기업 평판에 해로운 영향을 미칠 수도 있다. 따라서 네트워크 보안은 네트워크 운영 및 관리의 기본이다.

현재 우리가 사이버 군비 경쟁에 직면하고 있다는 것은 부인할 수 없다. 공격자들은 지속해서 네트워크를 공격하는 현명한 방법을 찾고 있으며, 보안 전문가는 알려진 공격과 가장 중요한 제로 데이 공격으로부터 네트워크를 보호하기 위한 새로운 조치를 개발하고 있다. 이러한 보안 조치의 예는 다음과 같다.

- 네트워크를 통과하는 패킷에서 데이터의 무결성과 기밀성을 보호하기 위하여 네트워크 트래픽, 특히 페이로드의 암호화
- 자격 증명을 사용하여 권한이 있는 사람에게만 액세스를 제한하는 권한 부여
- 예를 들어 보안 정책을 사용하여 액세스 제어를 통해 역할 및 권한에 따라 다른 사용자에게 다른 액세스 권한과 특권의 부여
- 악성 코드(예 : 트로이 목마, 랜섬웨어 등)로부터 엔드 시스템 보호하는 안티바이러스
- 미리 정의된 규칙에 따라 네트워크 트래픽을 허용하거나 차단하는 하드웨어 또는 소프트웨어 기반의 방화벽

그러나 암호화 키 및 로그인 자격 증명이 유출되어 네트워크가 모든 종류의 위협에 노출될 수 있다. 또한, 방화벽 및 안티바이러스의 방지 기능은 규정된 규칙 및 패치 세트에 의해 제한된다. 따라서 사이버 위협의 초기 증상을 감지하고 피해가 발생하기 전에 충분히 신속하게 대응할 수 있는 2차 방어선을 포함하는 것이 필수적이다. 이러한 시스템을 일반적으로 IDS/IPS (Intrusion Detection / Prevention Systems)라고 한다. IDS는 네트워크에서 악의적인 활동의 징후를 모니터링하며 크

게 오용 및 이상 기반 시스템의 두 가지 범주로 분류할 수 있다. 전자는 알려진 공격의 시그니처에 의존하지만, 후자는 침입이 정상적인 네트워크 동작과 매우 다른 동작을 보인다는 개념을 기반으로 한다. 따라서 이상 기반 IDS의 일반적인 목적은 이 표준에서 벗어난 것을 감지하기 위해 “정상 동작“을 정의하는 것이다.

네트워크 보안을 위한 ML 적용과 관련하여 대부분 작업이 침입 탐지를 위한 ML 적용에 초점을 맞추고 있다. 여기서 침입 탐지는 네트워크를 위협할 수 있는 모든 형태의 공격(예: 프로빙(probing), 피싱(phishing), DoS, DDoS 등)을 탐지하는 것을 말한다. 이것은 하나의 분류 문제로 볼 수 있다. 호스트 기반 침입 탐지 (예 : 악성 코드 및 봇넷 탐지)에 대한 많은 작업이 있지만 이러한 작업 대부분은 최종 호스트에서 수집된 추적 (때로는 상관관계에 있음)을 활용하기 때문에 이 주제를 다루지 않는다. 구체적으로 여기에서는 네트워크 기반 침입 감지에 초점을 맞추고 작업을 오용, 이상 및 하이브리드 네트워크 IDS의 세 가지 범주로 분류한다.

ML 기술	데이터셋	특징
지도 NN (offline)	• Normal • RealSecure Attack	TCP, IP, ICMP 헤더 필드, 페이로드
C5 DTs의 지도 앙상블 (offline)	KDD Cup	41개 특징
지도 NN과 C4.5 DT (offline)	KDD Cup	41개 특징
지도 NN (offline)	KDD Cup	35개 특징
지도 BN & CART (offline)	KDD Cup	Markov Blanket과 Gini rule을 사용한 특징 선택
지도 NB	KDD Cup	41개 특징
지도 C4.5 DT (offline)	KDD Cup	GA 기반 특징 선택
SVM, DT & SVM-DT의 지도 앙상블	KDD Cup	41개 특징
지도 C4.5 DT (online)	Normal: Reliability Lab Data	TCP, UPD, ICMP 헤더 필드
지도 앙상블 MPML	NSL-KDD	41개 특징
지도 TCM K-NN	KDD Cup	• 41개 특징 • Chi-square를 사용하여 선택한 8개 특징

표 21 ML 기반 오용 탐지(Misuse detection)에 관한 연구 동향

ML 기술	데이터셋	특징
비지도 계층적 SOM (offline)	KDD Cup	6 TCP 특징
지도 SVM (offline)	KDD Cup	GA를 사용하여 선택됨
비지도 개선 NN (offline)	KDD Cup	41개 특징
비지도 random forests (offline)	KDD Cup	서비스 형태로 레이블된 40개 특징
지도 커널 함수 (online)	from Abilene backbone network	패킷 수, 개별 IP 플로우 수
비지도 soft-margin SVM & OCSVM (offline)	KDD Cup Dalhousie U.에서 수집된 데이터	GA를 사용하여 선택됨
비지도 다중 분류기 (offline)	KDD Cup	29 features for HTTP 34 features for FTP 16 features for ICMP 31 features for Mail 37 features for Misc 29 features for Private & Other
지도 decision stumps with AdaBoost (offline)	KDD Cup	41개 특징
비지도 k-Means, C4.5 DT (offline)	KDD Cup	41개 특징
비지도 RF, ND, END (offline)	NSL-KDD	41개 특징
지도 RBF-SVM (offline)	Normal: Genoa U.의 말웨어	7 SDN OpenFlow 특징

표 22 플로우 특징 기반 이상 탐지(anomaly detection)에 관한 연구 동향

ML 기술	데이터셋	특징
비지도 2-tier SOM 기반 구조 (offline)	Normal: KDD Cup Attack: Nessus 스캔	패킷 헤더 및 페이로드
비지도 센트로이드 모델 (offline)	KDD Cup & CUCS	TCP의 페이로드
지도 단일 클래스 SVM의 지도 앙상블 (offline)	Normal: KDD Cup, GATECH Attack: CLET, PBA, Generic	페이로드
지도 SVDD (online)	Normal: Fraunhofer Inst. 페이로드 Attack: Metasploit	페이로드

표 23 페이로드 기반 이상 탐지(anomaly detection)에 관한 연구 동향

ML 기술	데이터셋	특징
RL: CMAC-NN (online)	프로토타입 응용	ping flood와 UDP 패킷 스톰 공격의 패턴
RL: Q-learning (online)	ns-2로 생성	혼잡, 지연, 플로우 기반
DL: DBN w/ AutoEncoder (offline)	KDD Cup	41개 특징
DL: DBN (offline)	NSL-KDD	39개 특징
DL: DNN (offline)	NSL-KDD	6개 기본 특징
DL: LSTM-RNN (offline)	KDD Cup	41개 특징
DL: Self-taught learning (offline)	NSL-KDD	41개 특징

표 24 침입 탐지를 위한 심층 학습 및 강화 학습에 관한 연구 동향

ML 기술	데이터셋	특징
지도 RBF-SVM (online)	KDD Cup	41개 특징
하이브리드 계층적 RBF (online)	KDD Cup	41개 특징
하이브리드 SOM w/J.48 (offline)	KDD Cup	SOM의 6가지 기본 특징 J.48의 41개 특징

표 25 하이브리드 침입 탐지를 위한 머신 러닝에 관한 연구 동향

4. 차기 연구 방향

4.1 실제적인 고품질 개방형 데이터셋의 확보

네트워크 프로필과 성능 메트릭을 모두 포함하는 대량의 고품질 데이터를 수집하는 것은 MLN의 가장 중요한 문제 중 하나이다. 그러나 레이블이 지정된 데이터를 충분히 수집하는 것은 오늘날의 머신 러닝 커뮤니티에서도 여전히 비용이 많이 들고 노동 집약적이다. 여러 가지 이유로, 네트워킹 도메인에 기존의 오픈 데이터 세트가 많더라도 연구원이 충분한 실제 추적 데이터를 획득하기는 쉽지 않다.

이러한 현실은 ImageNet과 같은 개방형 데이터 세트를 구성하는데 훨씬 더 큰 노력을 기울일 필요가 있다는 것을 나타낸다. 통합된 개방형 데이터 세트를 통해 성능 벤치마크는 연구원이 새로운 알고리즘 또는 아키텍처를 최신 알고리즘과 비교할 수 있는 표준 플랫폼을 제공하기 위해 꼭 필요하다. 이것은 반복 실험을 줄이고 학업 및 연구 충실도에 긍정적인 영향을 미칠 수 있다. 이러한 개방형 데이터셋은 MLN과 네트워킹 도메인의 추가 개발에 모두 이바지하며 공공 자원은 커뮤니티가 연구를 수행할 수 있도록 한다.

4.2 네트워크 관리의 단순화

최근 몇 년 동안 네트워크 관리를 단순화하기 위해 SDN과 같은 새로운 네트워크 아키텍처가 제안되었지만, 네트워크 운영자는 여전히 너무 많이 알고 있기를 기대받으며, 모니터링 소스를 통해 현재 네트워크 상태에서 네트워크가 어떻게 설계되었는지와 그들이 알고 있는 것을 상호 연관시킬 것을 기대받는다. 수동으로 복잡성과 씨름하여 이러한 요구사항을 관리하는 운영자는 (반) 자동화된 머신 러닝에서 얻을 수 있는 모든 휴식을 확실히 환영한다. ML이 네트워킹에서 널리 퍼지기 위해서는, ML 결과를 네트워크 운영자를 위해 실행 가능한 인사이트 및 보고서로 전송하는 주요 과제를 나타내는 “의미적 차이(semantic gap)”를 극복해야 한다.

이를 통해 네트워크 관리를 위한 반응형(reactive) 스타일에서 문제가 발생할 때 네트워크 관리자가 지도와 그래프를 확인해야 하는 방식에서 다양한 서비스 및 네트워크 지역에 대해 자동화된 보고서 및 알림이 생성되는 사전예방적(proactive) 방식으로 전환할 수 있다. 이것은 네트워크의 다른 부분에서 오는 다른 보고서들이 자동으로 상관되어 결합할 수 있다. 이를 위해서는 단순한 알림 및 시각화를 넘어 잠재적인 문제 소스를 식별할 수 있는 보다 실질적인 합성으로 나아간다. 또 다른 예는 측정을 보다 사용자 중심으로 만드는 것과 관련이 있다. 대부분 사용자는 QoS 대신 QoE에 더 관심이 있을 것이다. 즉, 네트워크의 현재 상태가 원시 QoS 메트릭보다는 애플리케이션과 서비스에 미치는 영향이다. 측정 목표의 개발은 traceroute, ping, BGP 등과 같은 다양한 도구와 프로토콜을 통해 수집된 통계를 제시하는 것뿐만 아니라 사용자에게 있는 다양한 지식을 통합해야 하는 부담이 있는 비즈니스 눈의 관점에서 이루어져야 한다.

4.3 네트워크 자원 관리

Cisco는 최번시(busy hour)와 평균 인터넷 트래픽 간에 상당한 차이가 있다고 한다. 2016년에는 최번시 인터넷 트래픽이 평균 인터넷 트래픽의 32% 증가에 비해 51% 증가했다[13]. 이러한 차이는 향후 5년 동안 더 커질 것으로 예상하며, Cisco는 최번시 트래픽의 증가율이 평균 인터넷 트래픽의 거의 1.5 배에 달할 것으로 예측한다.

이러한 동적 트래픽을 수용하기 위해 네트워크 사업자는 더 이상 최대 트래픽 요구사항에 따라 정적 자원 프로비저닝을 위한 CAPEX를 감당할 수 없다. 따라서 네트워크 사업자는 다양한 트래픽 수요에 따라 확장할 수 있는 동적 자원 할당을 사용해야 한다. ML은 수요 예측을 지원하고 네트워크 자원의 사전 프로비저닝 및 해제를 쉽게 하는 동적 자원 할당의 필수 부분이다. 또한, 상황에 맞는 정보를 ML에서 활용하여 예외적인 자원 수요를 예측하고 변동이 심한 환경에서 긴급 자원을 예약할 수 있다.

네트워크는 지원되는 애플리케이션과 서비스의 수와 다양성 측면에서 기하급수적인 성장을 경험하고 있다. 여기에는 대기 시간, 지터, 안정성, 가용성 및 이동성 측면에서 엄격하고 이기종의 QoS 요구사항이 있다. 네트워크 운영자는 네트워크의 모든 장치를 인식하지 못할 뿐만 아니라 모든 애플리케이션과 QoS 요구사항을 인식하지 못할 수 있다. 따라서 제한된 지식으로 효율적인 수락 제어 및 자원 관리 메커니즘을 고안하는 것이 어렵다. 기존 연구에 따르면 수락 제어와 자원 관리가 모두 학습 문제로 공식화될 수 있으며 ML은 성능을 개선하고 효율성을 높일 수 있다. 추가 단계는 수락 제어 및 자원 관리 전략을 네트워크 운영 경험에서 직접 학습할 수 있는지 탐색하는 것이다. 네트워크 경험과 관리 전략 사이의 복잡한 관계를 고려할 때 DL을 활용하여 네트워크의 입력과 출력 간의 고유한 관계를 특성화할 수 있다.

네트워크 조건의 불확실성과 역동성으로 인해 원칙 기반 휴리스틱 알고리즘으로 온라인 스케줄링을 수행하기가 어렵다. ML 커뮤니티에서 RL이 의사 결정 문제를 처리할 수 있는 강력한 능력이 있음이 입증되었다. 고도로 변화하는 네트워크 환경에서 탐색-활용(exploration-exploitation) 전략을 직접 적용하기는 쉽지 않지만, RL은 현재 네트워크 시스템의 적응형 알고리즘을 대체할 수 있는 후보가 될 수 있다. 또한, RL은 네트워크 상태에 따라 여러 가지 미확인 매개 변수를 적응적으로 할당해야 하는 문제에 매우 적합하다. 그러나 안정성, 신뢰성 및 반복성은 항상 네트워크 설계의 목표이지만 이러한 방법은 네트워크 시스템 자체에 새로운 복잡성과 불확실성을 도입한다.

또한, RL을 사용한 네트워크 스케줄링은 유연한 목적 함수 및 계층 간 최적화를 지원할 새로운 기회를 제공한다. 전통적인 휴리스틱 알고리즘으로는 불가능했던 학습 모델의 보상 함수를 변경하는 것만으로 최적화 목표를 변경할 수 있어 매우 편리하다. 또한, 시스템은 높은 수준의 애플리케이션 동작 또는 QoE 메트릭을 보상(reward)으로 인식할 수 있으며, 이는 네트워크 모델 없이 적응형 교차 계층 최

적화를 가능하게 할 수 있다. 실제로 효과적인 보상 기능을 설계하는 것은 간단하다. 가장 간단한 보상 설계 원칙은 극대화해야 할 직접적인 목표를 보상으로 설정하는 것이다. 그러나 정확한 최적화 목표를 포착하기가 어려운 경우가 많으며 결과적으로 불완전하지만 쉽게 얻을 수 있는 측정 항목이 된다. 대부분은 잘 작동하지만 때때로 바람직하지 않거나 심지어 위험한 행동을 초래할 수 있는 잘못된 보상 기능으로 이어진다.

4.4 SDN

SDN은 적응형 및 지능형 네트워크 프로빙(probing)을 가능하게 할 수 있다. 프로브는 네트워크 동작을 모니터링하고 네트워크 요소에서 측정값을 얻는데 사용되는 테스트 트랜잭션이다. 최적의 프로브 속도를 찾는 것은 많은 수의 장치, 다양한 측정 매개 변수 및 데이터를 기록하는 시간 간격이 짧으므로 향후 네트워크에서 엄청나게 큰 비용이 들 것이다. 적극적인 프로빙은 트래픽 오버헤드의 양을 기하급수적으로 증가시켜 네트워크 성능을 저하시킬 수 있다. 반대로, 보수적 프로빙은 몇 가지 중요한 이상 또는 중요한 네트워크 이벤트를 놓칠 위험이 있다. 따라서 성능 저하를 최소화하면서 트래픽 오버헤드를 목푯값 내로 유지하는 프로빙 속도를 조정하는 것이 필수적이다. SDN은 ML 기술을 활용하여 적응형 프로빙을 실현하는 완벽한 플랫폼을 제공할 수 있다. 예를 들어 결함을 예측하거나 이상을 감지하면 SDN 컨트롤러는 의심되는 장치를 더 빠른 속도로 검색할 수 있다. 마찬가지로 네트워크 과부하 동안 컨트롤러는 프로빙 속도를 줄이고 회귀에 의존하여 측정된 매개 변수의 값을 예측할 수 있다.

5. 결론

분명히 미래의 네트워크는 정보 액세스 및 공유를 위한 탁월한 기능을 제공하기 위해 트래픽 양과 연결된 장치의 폭발적인 증가를 지원해야 한다. 전례 없는 규모와 불확실성의 정도는 혼잡 제어, 트래픽 예측, 분류 및 라우팅과 같은 트래픽 엔지니어링 작업의 복잡성은 물론 결함 및 보안 공격에 대한 노출을 증폭시킬 것이다. 또한, 컴퓨터 네트워크의 다양성과 진화하는 특성으로 인해 모든 애플리케이션을 모두 처리하는 것은 불가능했다.

ML 기반 솔루션이 위 문단에서 언급한 많은 트래픽 엔지니어링 과제를 해결할 가능성을 보여주었다. 네트워킹 시스템의 이질성 때문에, 잠재적인 혁신을 위해 네트워킹 도메인에서 ML 기술을 포용하는 것이 필요하다. 그러나 ML 관련 경험이 부족하고 방향성이 불충분하여 네트워크 운영자와 연구자들이 이를 실천하기가 쉽지 않다.

현재 다양한 형태의 학습 모델이 지도 학습, 비지도 학습, 준지도 학습, 강화학습 등을 이용하여 네트워크 운영, 자율화, 자원 관리, 자원 할당, 보안 등의 문제를 해결하기 위해 연구되고 있다. 하지만 예상되는 데이터양, 장치 및 애플리케이션 수를 고려하여 확장성을 평가해야 한다. 반면에 결함 및 보안 관리를 위한 기존 ML 기반 접근 방식은 주로 단일 테넌트 및 단일 계층 네트워크에 중점을 둔다. 향후 네트워크에 대한 결함 및 보안 관리 프레임워크를 개발하려면 기존 ML 접근 방식을 확장하거나 다시 설계하여 다중 계층 네트워크의 다중 테넌시 개념을 고려해야 한다.

결론적으로, 네트워킹 기술과 AI 기술은 네트워크에서 점차 융합되어 ML과 DL 기술의 활용은 늘어날 것으로 판단된다. 따라서, 연구자뿐만 아니라 네트워크 운영자도 네트워크의 동작을 이해하기 위해 불가피하게 AI 기술을 숙지하여야 한다.

REFERENCES

[1] K. Schwab, "The Fourth Industrial Revolution: what it means, how to respond," World Economic Forum, 14 1 2016. [Online]. Available: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

[2] 글쓰는 부엉이, "4차산업혁명이란 무엇인가?," 2017. [온라인]. Available: https://brunch.co.kr/@jooshine/36.

[3] kjun.kr, "인공지능 머신러닝 딥러닝 무엇이 다를까?," 2017. [온라인]. Available: https://kjun.kr/481.

[4] R. Boutaba, M. A. Salahuddin, N. Limam, S. Ayoubi, N. Shahriar, F. Estrada-Solano and O. M. Caicedo "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities," in *Journal of Internet Services and Applications*, 2018.

[5] Rahulkishorebdm, "Machine Learning in Business Intelligence," 2020. [온라인]. Available: https://medium.com/@rahulkishorebdm/machine-learning-in-business-intelligence-6ed6980f37f9.

[6] R. van Loon, "Machine learning explained: Understanding supervised, unsupervised, and reinforcement learning," 2018. [Online]. Available: https://bigdata-madesimple.com/machine-learning-explained-understanding-supervised-unsupervised-and-reinforcement-learning/.

[7] wikipedia.org, "강화 학습," 2020. [온라인]. Available: https://ko.wikipedia.org/wiki/%EA%B0%95%ED%99%94_%ED%95%99%EC%8A%B5.

[8] 카카오 정책산업연구, "[카카오AI리포트]알파고를 탄생시킨 강화학습의 비밀," 2017. [온라인]. Available: https://brunch.co.kr/@kakao-it/73.

[9] Kumar Arun, Salau Ayodeji, Gupta Swati, and Arora Sandeep, "A Survey of

Machine Learning Methods for IoT and their Future Applications," in *Amity Journal of Computational Sciences (AJCS)*, 2018.

[10] 김태연, 고남석, 양선희, 김선미 "네트워크와 AI 기술 동향," 전자통신동향분석 *35권 제5호*, 10 2020.

[11] M. Wang, Y. Cui, X. Wang, S. Xiao and J. Jiang, "Machine Learning for Networking: Workflow, Advances and Opportunities," in *IEEE Network*, 2017.

[12] T. Mitchell, Machine Learning, McGraw Hill: 1997,

[13] Cisco. The Zettabyte Era: Trends and Analysis. 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html.

발 행 처 한국과학기술정보연구원
발 행 일 2020년 12월
주 소 (34141) 대전광역시 유성구 대학로 245
대표전화 042) 869-1004, 1234
팩 스 042) 869-1091
홈페이지 https://www/kisti.re.kr

비매품/무료
93560
9 788929 411596
ISBN 978-89-294-1159-6

네트워킹을 위한 AI 연구 동향

Trends in AI Researches for Networking

한국과학기술정보연구원
Korea Institute of Science and Technology Information
www.kisti.re.kr

본원
(34141) 대전광역시 유성구 대학로 245
TEL. 042) 869-1004, 1234
FAX. 042) 869-1091

분원
(32456) 서울특별시 동대문구 회기로 66
TEL. 02) 3299-6114
FAX. 02) 3299-6244