빅데이터 기말 프로젝트

랜덤 포레스트를 이용한 DDoS 공격 탐지

20210985

컴퓨터공학전공 노하림

문제 설명

네트워크 트래픽 데이터를 분석하여 **DDoS 공격을 탐지**하고 예방함으로써 **네트워크 보안을 강화하며, 시스템을 보호**하는 것을 목표로 한다.

문제 설명

DDoS(Distributed Denial of Service) 공격은 다수의 컴퓨터 시스템을 통해 특정 웹 서버나 네트워크 자원에 대량의 트래픽을 보내 정상적인 서비스 제공을 방해하는 사이버 공격이다.
이는 주로 네트워크 인프라를 마비시켜 합법적인 사용자가 서비스에 접근하지 못하도록 하는 목적으로 수행된다.

목적

네트워크 트래픽 데이터를 분석하여 DDoS 공격을 효과적으로 탐지하고, **정상 트래픽과 DDoS 트래픽을 구별하는 모델을 개발**하는 것이다.
이를 통해 DDoS 공격을 조기에 탐지하고 차단할 수 있는 시스템을 구축하여 네트워크 인프라의 안정성과 보안을 강화할 수 있다.

중요한 이유

1. 서비스 중단 방지

DDoS 공격은 웹 서버와 네트워크 인프라의 가용성을 저하시켜 서비스 중단과 금전적 손실을 초래한다. 이를 조기에 탐지하고 차단하여 서비스 중단을 방지하는 것이 중요하다.

2. 데이터 보호 및 보안 강화

DDoS 공격은 다른 형태의 사이버 공격과 결합될 수 있어 데이터 침해를 초래할 수 있다. DDoS 공격을 예방하고 차단함으로써 데이터를 보호하고, 시스템을 보호할 수 있다.

데이터

사용된 데이터 : CIC-IDS-2017 데이터셋 데이터셋 링크
데이터 획득 방법 및 링크 : Canadian Institute for Cybersecurity에서 제공. 네트워크 보안 연구 및 학습을 위해 공개

데이터 설명

이 프로젝트에서 사용된 데이터는 CIC-IDS-2017 데이터셋의 일환으로, 네트워크 트래픽 로그를 포함하고 있으며, 정상 트래픽과 다양한 유형의 공격 트래픽을 포함한다. 해당 데이터셋에는 225,711개의 샘플이 있다. 이 프로젝트에서는 DDoS 공격에 초점을 맞추어 분석을 진행한다.

데이터 구조

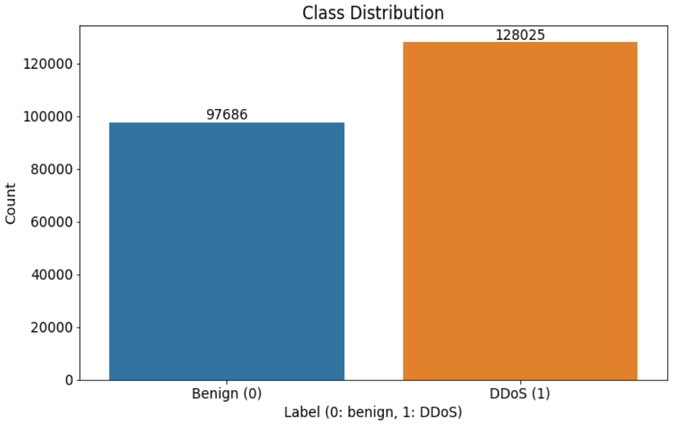
특성 (Features)

총 78개의 특성으로 구성되어 있다.

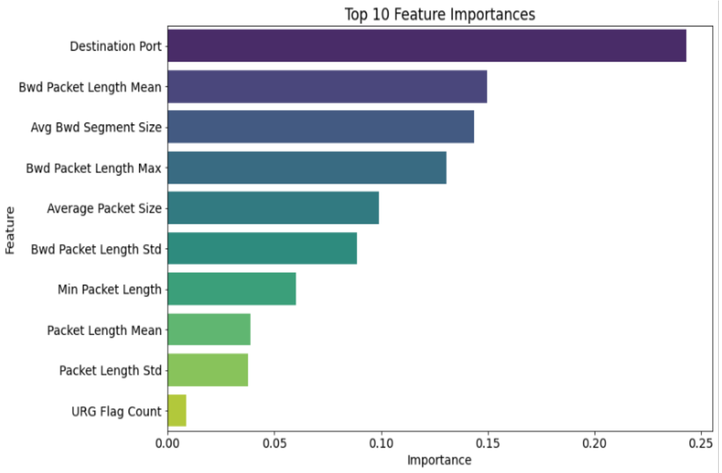
이 프로젝트에서는 scikit-learn에서 제공하는 특성 선택 기법인 **SelectKBest**를 사용하여 10개의 특성을 선택하고 사용한다.

레이블 (Label)

트래픽 유형 (0 : 정상 트래픽 / 1 : DDoS 공격)



레이블 분포 시각화



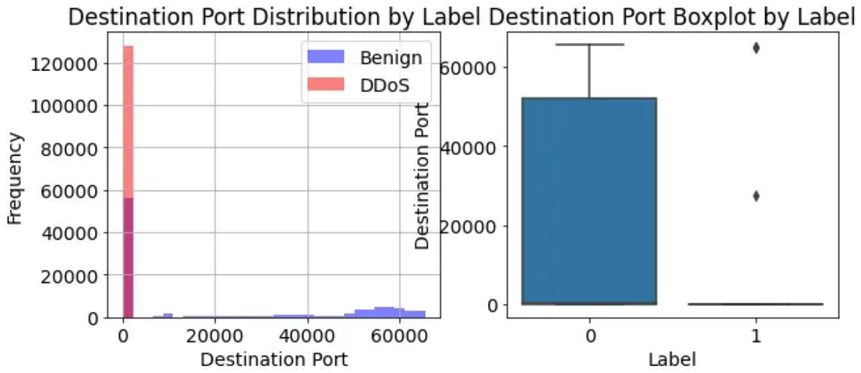
특성 중요도 시각화

분석 방법

	항목의 세부 내용
1. 데이터 전처리	1. 데이터 불러오기 및 정리 : CSV 파일을 Pandas 데이터프레임으로 불러온 후, 열 이름에서 공백을 제거하여 데이터 정리 2. 결측값 처리 : 무한대 값이 있는 행을 NaN으로 대체 후 삭제, 결측값은 평균값으로 대체 3. 레이블 인코딩 : Label에 열의 값 DDos는 1로, benign을 0으로 변환하여 이진 분류 수행 가능하도록 함 4. 데이터 스케일링 : 특성 데이터를 StandardScaler를 사용해 정규화함
2. 모델 학습	1. 특성 선택 : SelectKBest와 f_classif 기법을 사용하여 가장 중요한 특성 10개를 선택 2. 데이터 분할 : 전처리된 데이터를 학습 데이터와 테스트 데이터로 8:2 비율로 분할 3. 모델 학습 : RandomForestClassifier를 사용하여 학습 데이터로 모델을 학습
3. 모델 평가	1. 성능 지표 계산 및 시각화 : 테스트 데이터에 대해 모델의 정확도(accuracy), 재현율(recall), 정밀도(precision), F1 점수(f1 score), Matthews 상관계수(MCC)를 계산 2. PCA를 사용한 시각화 : PCA를 활용하여 데이터를 2차원으로 시각화하여 데이터의 패턴을 직관적으로 파악하도록 함

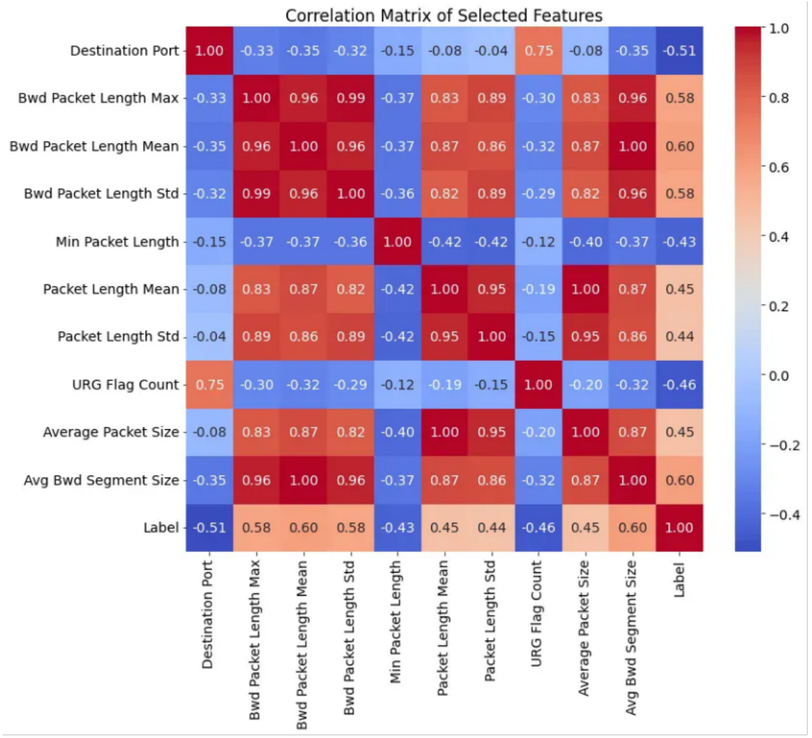
분석 결과

Destination Port Distribution 특성 분포



- DDos 트래픽은 대부분 매우 낮은 포트 번호에 집중
- DDos 공격으로 잘 알려진 특정 포트 (예: 80번 HTTP, 443번 HTTPS 등)를 대상임을 시사함
- 양성 트래픽은 넓은 범위의 포트에 분산
- 왼쪽 박스플롯은 넓은 사분위 범위를 보이며 이는 다양한 포트를 사용한다는 것을 의미

상관관계 행렬



레이블(Label)과의 상관관계

- 'Avg Bwd Segment Size'와 'Bwd Packet Length Mean'이 레이블과 가장 높은 양(0.60)의 상관관계를 보이며 특성이 증가할 때 DDoS일 가능성이 높아짐을 의미
- 'Destination Port'는 레이블과 강한 음의 상관관계(-0.51)를 가짐. 즉, 목적지 포트 번호가 낮을수록 DDoS일 가능성이 높음

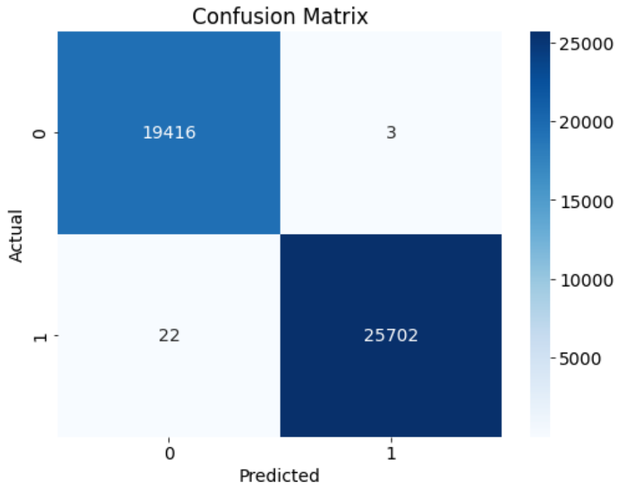
분석 결과

성능 지표

Metric	Score
Accuracy	0.999446
Recall	0.999145
Precision	0.999883
F1 Score	0.999514
MCC	0.998871

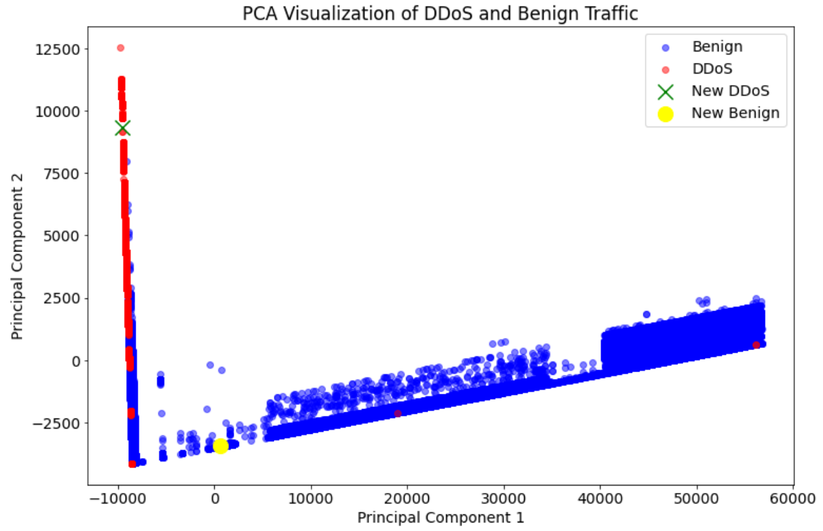
- 모델의 정확도, 재현율, 정밀도, F1 점수, MCC가 모두 매우 높은 값을 나타냄

혼동 행렬 시각화



- 모델이 25704개의 DDoS 트래픽과 19416개의 정상 트래픽을 정확히 탐지함
- 모델이 소수의 False Positive와 False Negative를 보이고 있지만, 그 수가 매우 적음

PCA



- PCA를 통해 시각화된 그래프에서 파란색(정상 트래픽)과 빨간색(DDoS 트래픽) 점들이 명확하게 구분됨
- 초록색 'X'로 표시된 새로운 DDoS 샘플은 기존 DDoS 클러스터 내에 있어 DDoS 공격으로 분류

결론

참고문헌
- "분산 서비스 거부 (DDoS) 공격: 정의, 영향 및 완화 전략" - Juniper Networks
- "Applied Multivariate Statistical Analysis" - Richard A. Johnson, Dean W. Wichern
- 랜덤 포레스트 알고리즘을 이용한 신용평가모형 구축 - 박경욱, 이승주

01

프로젝트 요약

- 이 프로젝트는 네트워크 보안을 강화하기 위해 DDoS 공격을 탐지하고 분류하는 모델을 개발하는 것을 목표로 함.
- CIC-IDS 2017 데이터셋을 사용하여 전처리를 거친 후, 랜덤 포레스트 분류기를 학습하여 모델을 구축함.
- 성능 지표를 사용하여 모델의 성능을 평가하고 예측을 시각화하여 모델의 신뢰성을 확인함.

02

프로젝트 결론

- 랜덤 포레스트를 이용한 DDoS 공격 탐지 모델이 높은 정확도와 성능을 보여줌으로써, 실제 시나리오에서 유용하게 활용될 수 있음을 입증함.
- DDos 예측을 통해 네트워크 보안을 강화하고 데이터를 보호할 수 있음.