【서식 3-1】 캡스톤디자인 과제 수행 결과보고서 (※ 학생 작성)_ 팀용

기업연계형 캡스톤디자인 교과목 과제 수행 결과보고서

과제 유형	■ 기업연계기반			
과제명	세션 슬라이싱 기법을 활용한 CNN 기반 악성 트래픽 분류 연구			
팀명	컴융 고지대			
수강 교과목명	캡스톤 디자인 II		교과목 학수번호	DCSS452(00)
교과목 담당교수	소 속	컴퓨터소프트웨어학과	성 명	서민석
	E - mail	mins@korea.ac.kr	교내전화	044-860-1379
지도교수	소 속	컴퓨터소프트웨어학과	성 명	김명섭
	E - mail	tmskim@korea.ac.kr	교내전화	044-860-1347
산업체 참여 인력(PM)	소 속	㈜하잎아이피	성 명	박재원
	E - mail	jwpark@hipe-ip.net		
산업체 역할 (자문내용)	• 보안 산업 현장에서 요구되는 실제 탐지 기술의 필요성과 적용 가능성에 대해 피드백을 제공함. • 연구 결과가 현업 환경에 맞게 활용될 수 있도록 실무적인 관점을 제시함.			

구분		성명	학과	학년	학번	E - mail
참여 학생	팀장	양지윤	**컴퓨터소프트웨어학과**	**4**	2022270649	didwldbssla@naver.com
	팀원	정고은	**컴퓨터소프트웨어학과**	**4**	2022271329	rhdms6552@naver.com

위와 같이 규정에 의해 과제를 완료하였음을 결과보고서로 제출합니다.

2026. 5. 21.

지도교수: 김명섭 (인 또는 서명)

대표학생: 양지윤 (인 또는 서명)

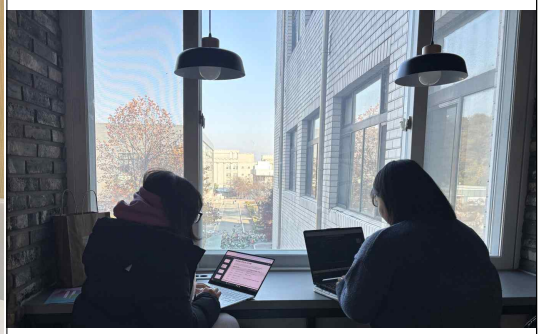
고려대학교 세종 SW중심대학사업단 귀하

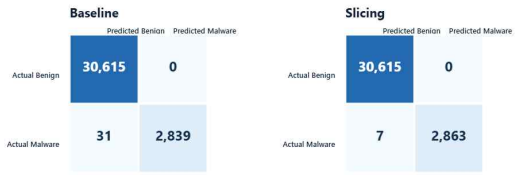
작품과제명	세션 슬라이싱 기법을 활용한 CNN 기반 악성 트래픽 분류 연구
과제 개요	○ 과제 선정 배경 - 최근 네트워크 기반 사이버 공격과 악성코드 유포가 증가하면서 악성 트래픽 탐지 기술의 중요성이 커지고 있음. - 기존 시그니처 기반 탐지 방식은 새로운 형태의 공격이나 변형된 악성코드에 대한 대응에 한계가 존재함. - 딥러닝 기반 네트워크 트래픽 분류 연구가 활발히 진행되고 있으며, 특히 CNN을 활용한 악성 트래픽 분류 모델이 높은 정확도를 보이고 있음. - 기존 연구에서는 세션의 앞부분 데이터만 사용하는 방식이 주로 활용되었으나, 세션 전체의 특징을 충분히 반영하지 못한다는 한계가 존재함. ○ 과제의 필요성 - 짧은 세션에서는 고정 길이 입력을 위해 과도한 패딩이 발생하여 학습 효율이 저하될 수 있음. - 기존 방식은 세션 중간 및 후반부의 중요한 트래픽 특징 정보를 반영하지 못하는 문제가 있음. - 실제 네트워크 환경에서는 다양한 길이와 형태의 트래픽이 발생하므로, 보다 일반화된 입력 방식이 필요함. - 세션의 앞·중간·뒤 구간을 함께 활용하는 슬라이싱 기법을 적용함으로써 악성 트래픽의 특징을 보다 효과적으로 학습할 수 있는 모델이 요구됨.
과제 내용	○ 과제 구성 - USTC-TFC2016 데이터셋을 활용하여 정상 및 악성 트래픽 데이터를 수집하고 전처리를 수행함. - 기존 논문의 CNN 기반 악성 트래픽 분류 모델을 구현하여 기본 성능을 재현함. 세션 전체를 활용하는 슬라이싱 기법을 적용하여 Front, Mid, Back 영역 데이터를 추출함. - 추출된 데이터를 RGB 3채널 형태로 구성하여 CNN 입력 데이터로 활용함. - 기존 방식과 제안 방식의 성능을 비교·분석하여 개선 효과를 검증함. ○ 과제 주요 특징 - 세션 앞부분만 사용하는 기존 방식과 달리 세션 전체 구간의 특징 정보를 반영함. - 짧은 세션에서 발생하는 과도한 패딩 문제를 완화하여 데이터 활용 효율을 높임. - Front, Mid, Back 구간을 활용하여 다양한 위치의 악성 트래픽 특징을 학습할 수 있도록 설계함. - Accuracy, Precision, Recall, F1-score 등 다양한 평가 지표를 통해 성능을 검증함. - 실시간 악성 트래픽 탐지 시스템에 적용 가능한 CNN 기반 분류 모델 구현을 목표로 함.
결과물의 활용방안 및 기대효과	- CNN 기반 악성 트래픽 분류 모델을 통해 네트워크 보안 환경에서의 악성코드 탐지 정확도를 향상시킬 수 있음. - 세션 슬라이싱 기법을 활용하여 다양한 길이의 네트워크 트래픽에서도 안정적인 분류 성능을 기대할 수 있음. - 실제 보안 산업 환경에서 활용 가능한 실시간 악성 트래픽 탐지 시스템 연구 기반으로 활용 가능함.

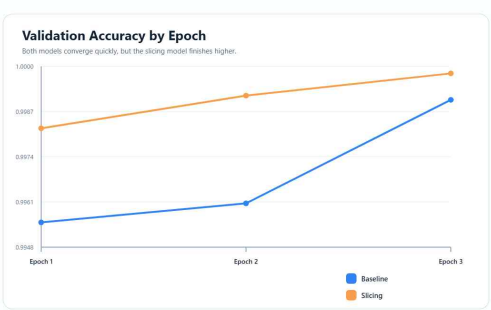
	- 향후 네트워크 침입 탐지 시스템(NIDS) 및 보안 관제 시스템 분야에 응용 가능성이 있음.

	구분	성명	과제 참여 내용(역할)
수행 방법	팀장	양지윤	세션 슬라이싱 기반 입력 구성 전처리 및 CNN 모델분석
	팀원	정고은	세션 슬라이싱 기반 입력 구성 전처리 및 CNN 모델 분석
	팀원		
	팀원		
	팀원		
	팀원		

결과물







Visualization Summary

Strategy	Accuracy	Precision	Recall	F1	Malware Misses
Baseline	0.999074	0.999494	0.994599	0.997032	31
Slicing	0.999791	0.999886	0.998780	0.999332	7

Key takeaway

- Slicing improved accuracy by 0.000717.
- Slicing improved macro recall by 0.004181.
- Malware false negatives dropped from 31 to 7.