

안드로이드용 현대 블루링크 앱의 데이터 분석을 통한 사용자 검색 장소 재구성

단국대학교 컴퓨터보안 및 운영체제 연구실

학부연구생 정연수

INDEX

01

연구 배경

02

제안 기법

03

실험 및 평가

04

결론 및 향후 연구



01

연구 배경

커넥티드 카의 대중화

- ❖ 차량과 연계된 다양한 데이터가 축적
- ❖ 차량 제조사가 제공하는 차량 연동 앱(Car Companion App, CCA)의 보편화
- ❖ 디지털 포렌식 측면에서의 활용 가능성

Types of V2X communication



[출처]: <https://www.nearbycomputing.com/v2x-technology/>

-4-

지도 타일의 포렌식 활용 가능성 탐색

❖ 네덜란드 포렌식 연구소 연구 결과

- 차량 내비게이션 시스템에서 생성된 지도 타일을 분석하여 최근 이동 경로 추정
- Android Automotive OS 기반 시스템을 대상
- map_cache.db를 복호화하여 지도타일 획득
- 타일 생성 조건 및 시간 정보를 포함한 분석이 미흡



[출처]: <https://github.com/NetherlandsForensicInstitute/gmaps-cache-db>



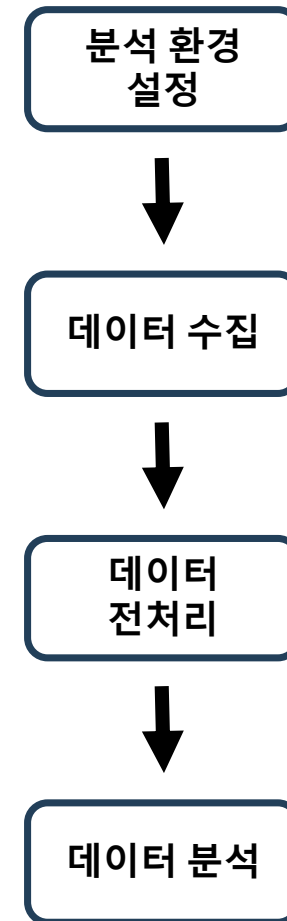
02

제안 기법

제안 기법

- ❖ 국내 CCA 중 블루링크의 지도타일 획득과 분석
- ❖ 지도 타일 생성 조건을 명시적 검색 행위로 제한
- ❖ 제한된 환경에서 생성되는 지도 타일 분석

번호	시간	목적지	검색 시도 장소
1	09:00	포항역 KTX	단국대학교
2	09:10	여수공항 국내선	
3	09:20	울릉도독도 해양연구소 주차장	
4	09:30	CU 백령도점	
5	09:40	죽전역 수인분당선	
6	09:50	포항역 KTX	





03

실험 및 평가

분석 환경 설정

❖ 디바이스 루팅

- 앱 데이터 수집을 위한 권한 획득

❖ 블루링크 루팅 탐지 로직 우회

- Frida를 통해 루팅 탐지 로직을 우회함.
- 루팅되지 않은 디바이스와의 교차 검증을 통해 기능이 정상적으로 동작하는 것을 확인

데이터 수집

❖ 앱 데이터 획득

- ADB(Android Debug Bridge)를 이용하여 블루링크 앱 데이터를 획득

❖ 앱 데이터 내에 캐시 파일 분석을 통해 지도 타일 획득

The diagram illustrates the process of extracting map tiles from app cache data. It consists of three main components:

- File Tree:** A directory structure showing the location of cache files. The path `Cache_Data (453)` is highlighted.
- Table:** A table listing the files in the `Cache_Data` directory. The table has two columns: `Name` and `Modified Time`. The file `018a8333b179dc80_0` is highlighted.
- Data List:** A list of extracted tile data. The first line is `1/0/https://tiles.routo.com/tile/roadmap_half_basic/v1/16/55911/25444.webpRIFF`, where `16/55911/25444` is highlighted in red. Other lines include `WEBPVP8`, `SjmM`, `SjmF'+I`, `rk.M`, `SjmM`, `SjmM`, `SjmM`, `rn2!`, `SjmM`, `SjmM`, `&QC_3`, `SjmM`, `~ABu`, `+SjmM`, `<+LX`, `:n!O`, `4mP9`, `of3hK`, and `1N4*`.

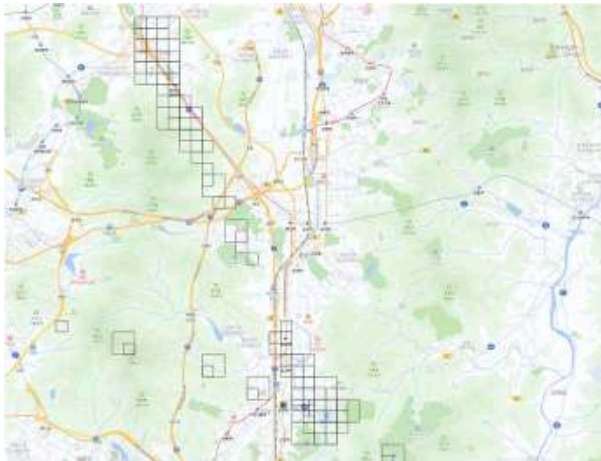
Arrows indicate the flow of data from the file tree to the table, and from the table to the data list. A red box highlights the extracted tile data, and a red text label `[(Z, X, Y), mtime]` 획득 is shown next to it.

데이터 전처리 & 군집화

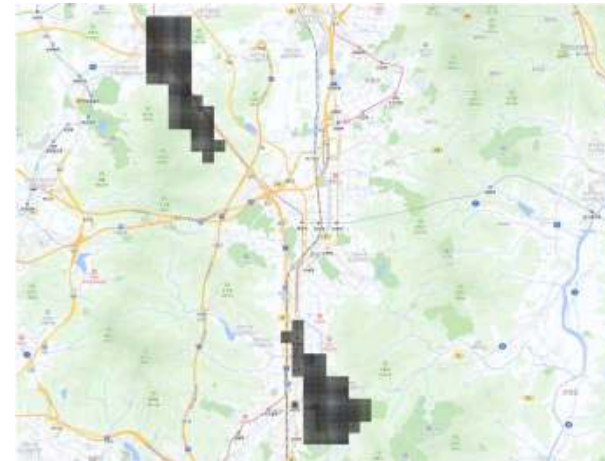
❖ 필터링

- 분석 목적에 무관한 노이즈 데이터 제거
- 줌 레벨 단일화

필터링 이전



필터링 이후



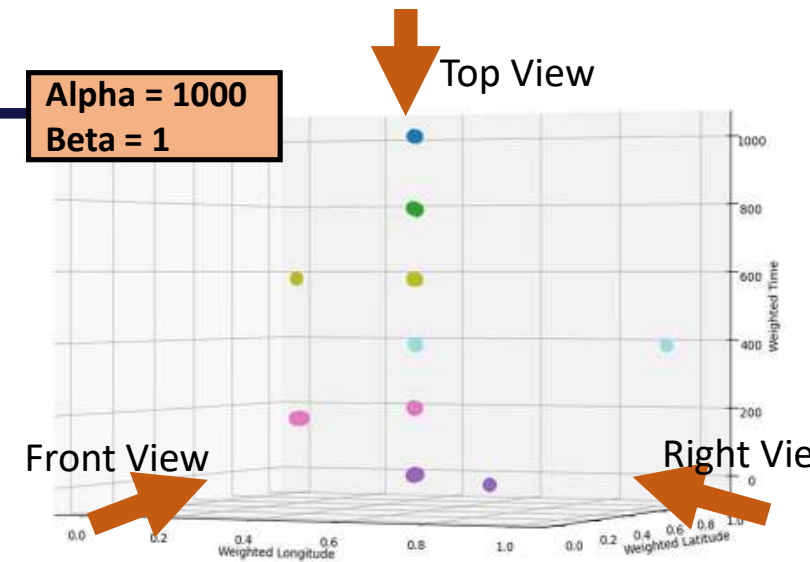
❖ 정규화

- Min-Max 정규화 이후 가중치 부여

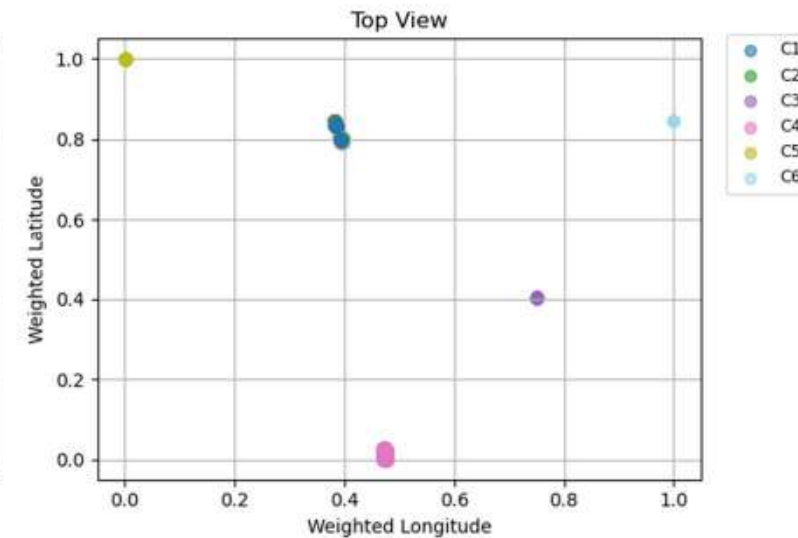
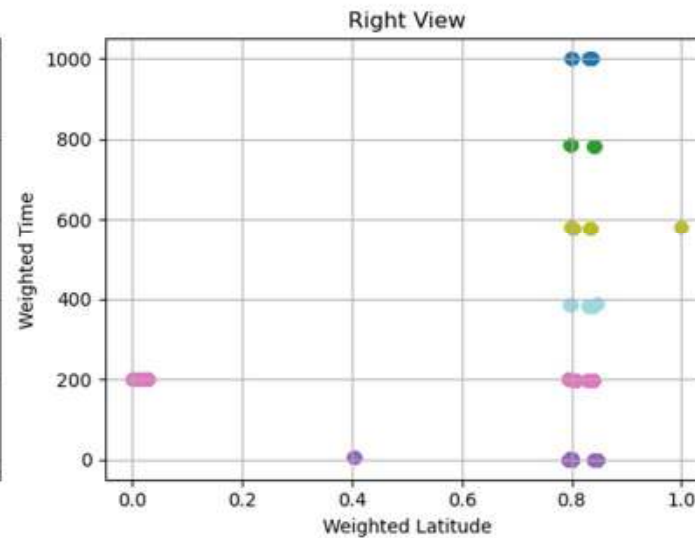
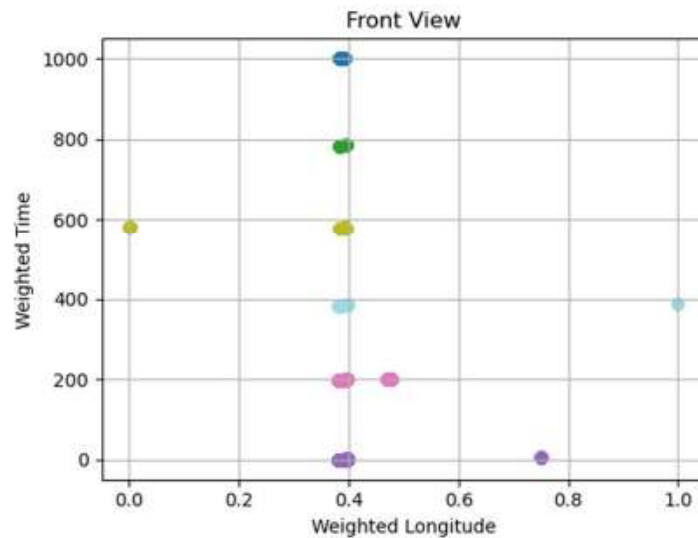
❖ 군집화(계층적 군집화 기법)

데이터 분석 - 시각화

- ❖ 시간에 대한 가중치(alpha)를 높게 설정
- ❖ 명시적 검색 행위마다 특정 위치에 대한 지도 타일 생성
- ❖ 재검색은 수정 시간을 변화시키지 않고
검색 장소에 대한 지도 타일도 생성하지 않음



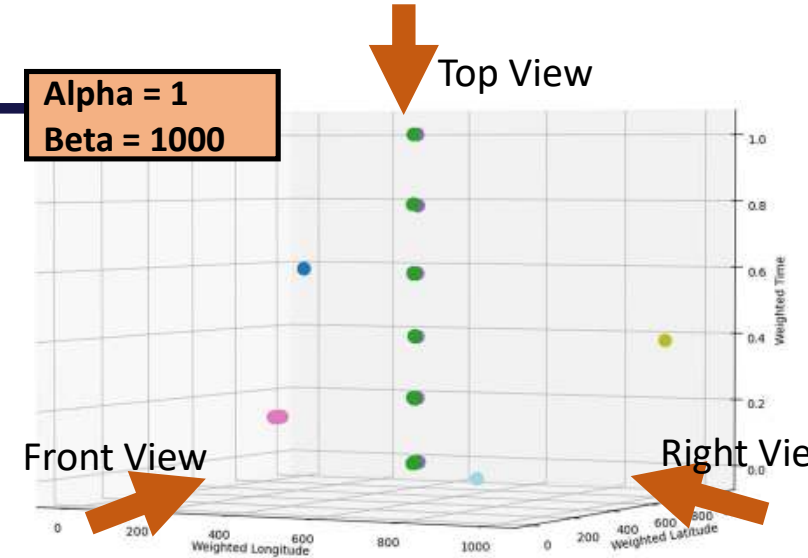
Three View drawing ($\alpha=1000, \beta=1$)



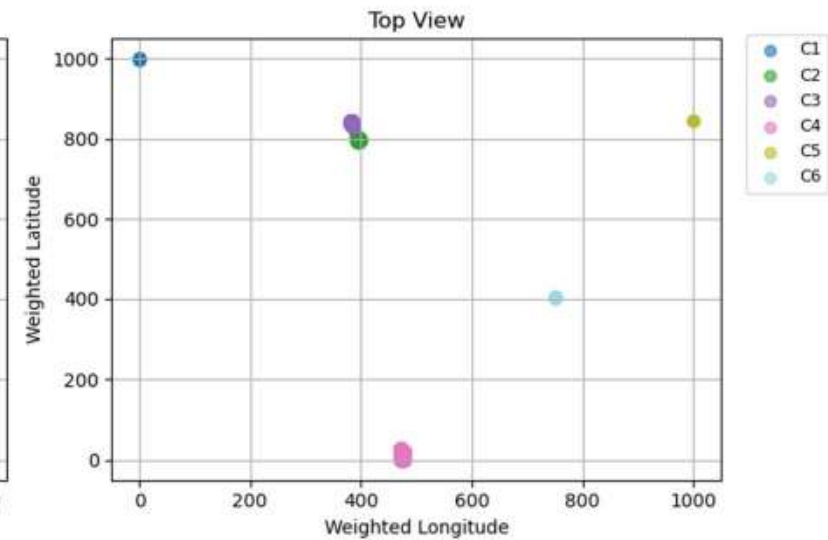
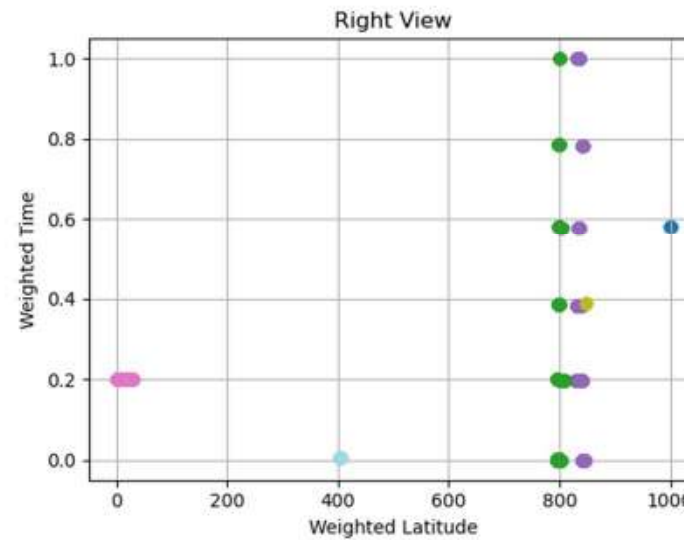
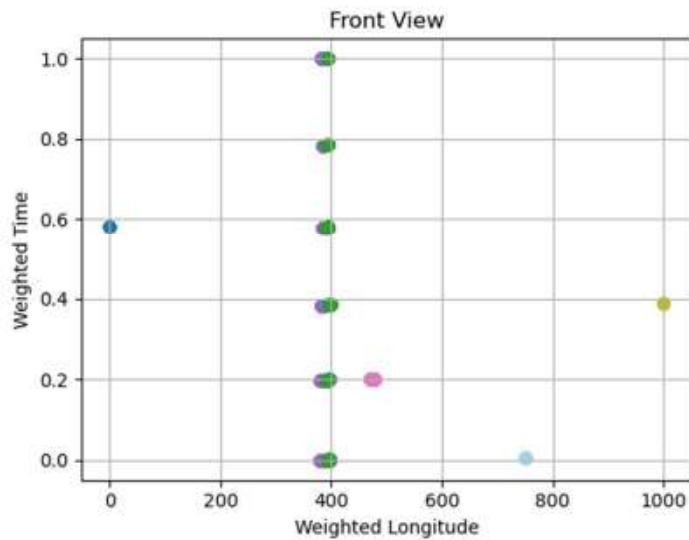
데이터 분석 - 시각화

❖ 공간에 대한 가중치(beta)를 높게 설정

Alpha = 1
Beta = 1000



Three View drawing ($\alpha=1, \beta=1000$)



실험 평가

❖ 의의

- CCA 기반 지도 타일 데이터 분석 시도
- 지도 타일 데이터의 시간 정보 활용을 통해, 사용자 행위 재구성 가능성 검증
- 명시적 검색 행위에 따라 생성되는 3가지 위치 정보 식별

❖ 한계

- 지도 타일 자체의 제한 사항
- 실험적 파라미터 설정

04

결론 및 향후 연구

결론 및 향후 연구

❖ 결론

- 사용자의 명시적 검색 행위에 의해 생성되는 아티팩트 확인
- 시간 정보를 통합한 분석을 통해 사용자 행위 재구성 가능

❖ 향후 연구 방향

- 다양한 지도 타일 생성 조건에 따른 패턴을 파악하고자 함.
- 제한되지 않은 환경의 데이터를 분석하여 일반화
- 다른 데이터와 통합 분석을 진행하여 신뢰도를 높이하고자 함.

Thank you

Q&A
