

Time Is Running Out

Assessing Temporal Privacy of Privacy Zones in Fitness Tracking Social Networks

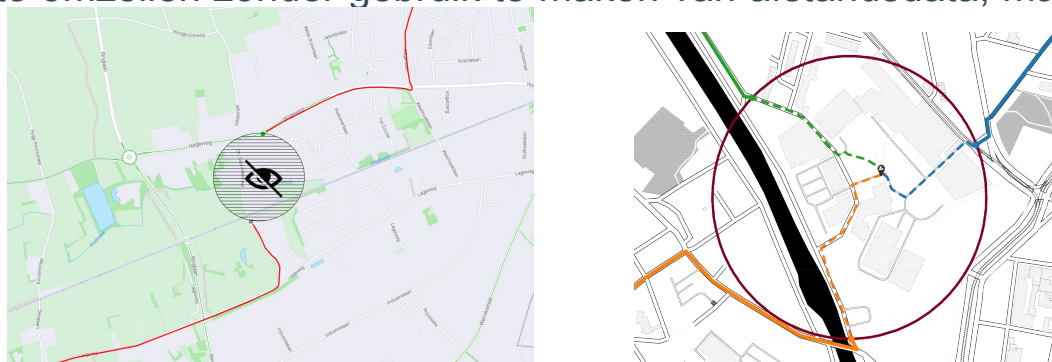
Situering

Fitnesstrackers zoals Strava zijn niet meer weg te denken uit deze moderne wereld. Dit zijn sociale netwerken die sportactiviteiten zoals lopen en zwemmen kunnen registreren, en delen met vrienden. Deze brengen echter ongewilde privacy bezorgdheden met zich mee. Gedurende deze thesis wordt onderzoek gedaan naar het ongewild vrijgeven van persoonlijke locaties (woonlocaties, militaire basissen, ...) ondanks de maatregelen van Strava.



Vraagstelling

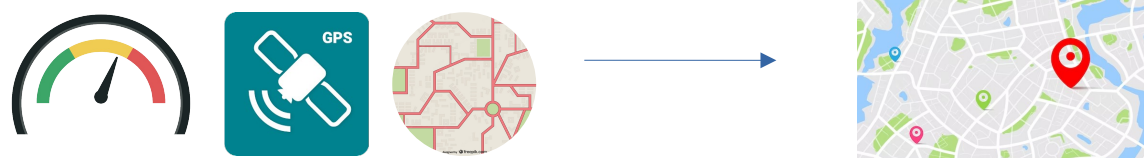
- Strava maakt gebruik van *Endpoint Privacy Zones* (EPZ) om gevoelige locaties te verbergen. Dit mechanisme bestaat eruit om alle routesegmenten binnen een bepaalde radius te verbergen. De vraag is of het mogelijk is om deze privacy zone te omzeilen zonder gebruik te maken van afstandsdata, maar door gebruik te maken van snelheidsdata.



Endpoint Privacy Zones

Werkwijze

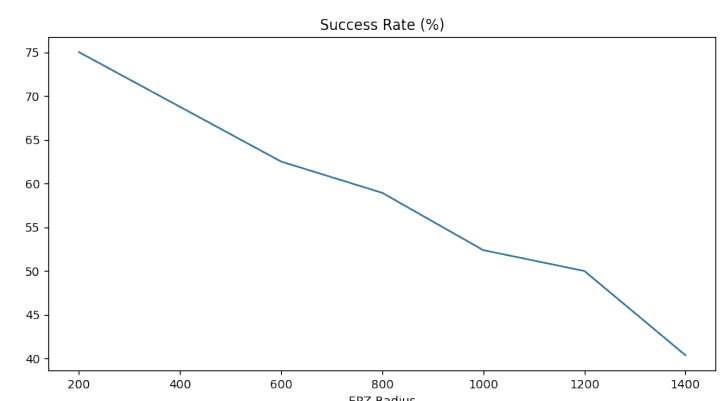
- Aan de hand van snelheden buiten de EPZ en de **totale gemiddelde snelheid**, wordt de totale afgelegde afstand bepaald. Via **GPS-coördinaten** wordt kan ook de totale afstand buiten de EPZ berekend worden. Beide afstanden afgetrokken van elkaar geven de afstand binnenin de EPZ. Deze afstand kan met behulp van het **wegennetwerk** gebruikt worden om de verborgen route te reconstrueren.



Mechanisme Aanval

Resultaten

- Het is zeker mogelijk om in een groot deel van de cases via deze gedachtengang gevoelige locaties te achterhalen. Afhankelijk van de omvang van de zone kan een succes rate van 75% bekomen worden. Dit wil zeggen dat voor 75% van de gevallen de locatie kan bepaald worden tot op 22,95m nauwkeurig.
- De precisie van een aanval gaat echter drastisch achteruit bij het verhogen van de grootte van de EPZ.



Resultaten aanval in functie van grootte EPZ

Student: W. Deleu

Promotor: dr. ir. S. Volckaert

Co-Promotor: ing. K. Dhondt, ing. A. Andries, ing. J. Vinck