

Bureau d'étude : Économie Numérique et Utilisation des Données

Attaques par inférence sur traces de mobilité

15 mars 2019

SCHERRER Matthieu
DESLANDES Benoît

1 Visualisation, Preproressing et premières idées

1.1 Preprocessing

Avant de pouvoir visualiser, nous avons du reformater les fichiers ID2 et ID3. Notamment, il a fallu les trier dans l'ordre chronologique et ajouter des virgules pour séparer les valeurs.

Après une première visualisation, nous avons repéré certains points aberrants, que nous avons décidé de retirer pour qu'ils n'interfèrent pas avec le clustering.

Dans le fichier ID2, on retire les points aberrants $(38.00^\circ; -123.852^\circ)$ et $(37.789^\circ; -122.597^\circ)$, car dans les deux cas l'individu est dans l'eau puis de retour sur la Terre ferme quelques secondes plus tard. Au sud, la fréquence des points est étrange, mais nous pensons qu'il faut tout de même les prendre en compte.

Dans le fichier ID3, nous suspectons les points $(37.86^\circ; -122.247^\circ)$, et $(37.508^\circ; -122.25^\circ)$ d'être aberrants. Dans le premier cas, le point est entouré de mesures proches dans le temps à un autre endroit, c'est donc une erreur du GPS. Dans l'autre, le point n'a pas de voisin temporel proche, le chauffeur était donc peut-être bien présent à cet endroit à ce moment, mais sans point supplémentaires nous décidons tout de même d'enlever cette position.

1.2 Premières inférences

Ces premières visualisations nous permettent d'ores et déjà d'obtenir quelques informations sur les trois individus. Le premier individu semble vivre et travailler dans la région toulousaine, et voyage fréquemment à Paris, sans doute pour le travail.

Au vu de leur temps passé sur la route et à l'aéroport de San Francisco, nous pouvons affirmer que les individus 1 et 2 sont chauffeurs de taxi dans cette région.

2 Attaque Begin-End

2.1 Attaque BE de l'utilisateur 1

Dans un premier temps, nous effectuons une attaque Begin-End sur les données GPS des utilisateurs. Ce type d'attaque consiste à identifier les points d'intérêt d'un individu en étudiant les moments d'immobilité temporelle et spatiale de celui-ci. Pour ce faire, nous avons utilisé les classes préimplémentées en Java, et avons réalisé une méthode effectuant l'attaque.

Les clusters obtenus par cette méthode sont régis par deux paramètres. Le premier est la **résolution spatiale**, c'est-à-dire la distance entre deux points maximale telle que l'on considère l'utilisateur immobile. Le second est la **résolution temporelle**, qui est la durée minimale pendant laquelle l'utilisateur doit respecter le premier critère pour compter comme un cluster.

Une fois les clusters obtenus, un nouveau clustering est réalisé sur les points obtenus. En effet, sans ce traitement, nous aurions par exemple un nouveau cluster à chaque nuit chez soi. Le post-traitement permet de fusionner toutes ces nuits en un seul point d'intérêt sur la maison de l'individu.

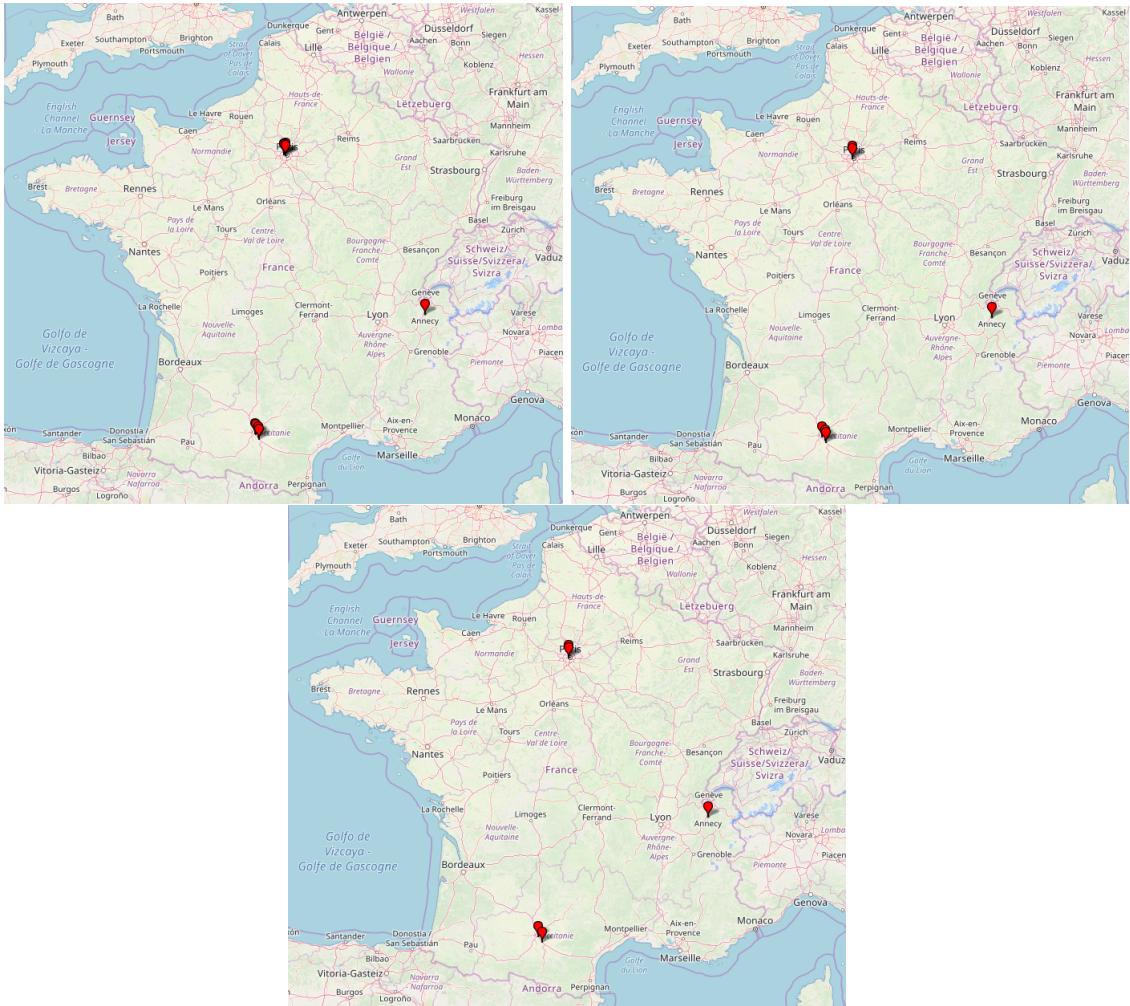


FIGURE 2.1 – Zones d'intérêt de l'utilisateur 1 pour un temps où l'immobilité est considérée à 5 minutes, 10 minutes et 20 minutes, pour une distance de 1km

Comme nous pouvions l'imaginer, augmenter la résolution temporelle diminue le nombre de clusters, car nous devenons plus exigeants sur la définition d'un cluster. Dans un cas à limite temporelle de 5 min, nous observons 8 clusters, puis 6 clusters pour 10 min et finalement 5 clusters pour 20 min. Par exemple, le cluster central à Toulouse qui apparaît dans le premier cas correspond à l'endroit où l'utilisateur effectue ses courses, et disparaît donc dans le dernier cas. On constate tout de même qu'à l'échelle de la France, les villes d'intérêt de l'individu considéré demeurent identiques. C'est l'information sur les lieux d'intérêts dans ces villes qui est modifiée.

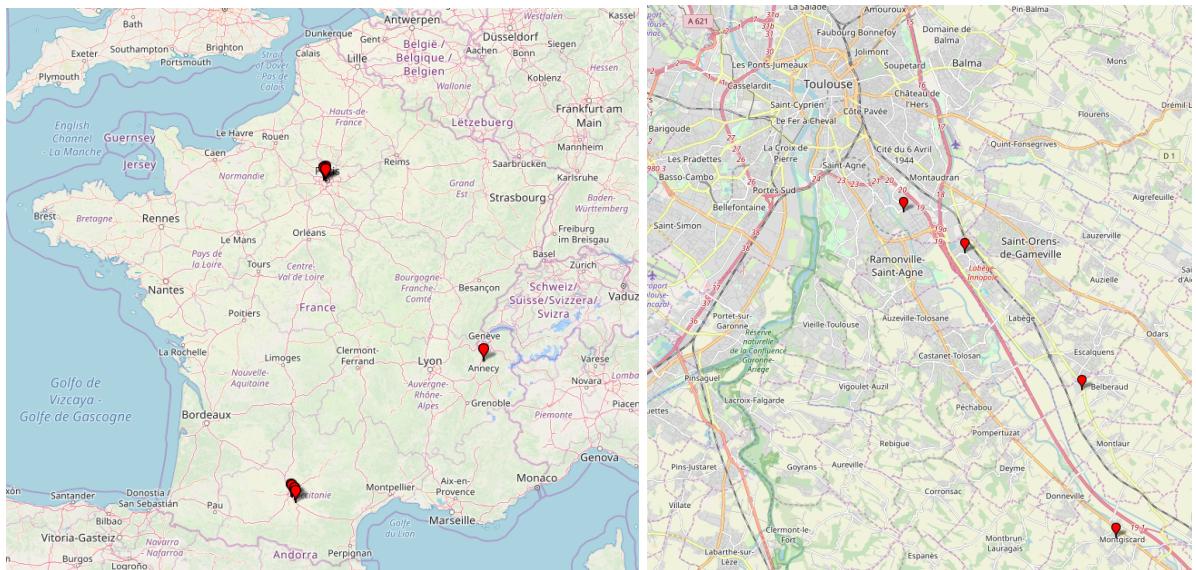


FIGURE 2.2 – Zones d'intérêt de l'utilisateur 1 pour un temps où l'immobilité est considérée à 5 minutes, pour une distance de 1 km

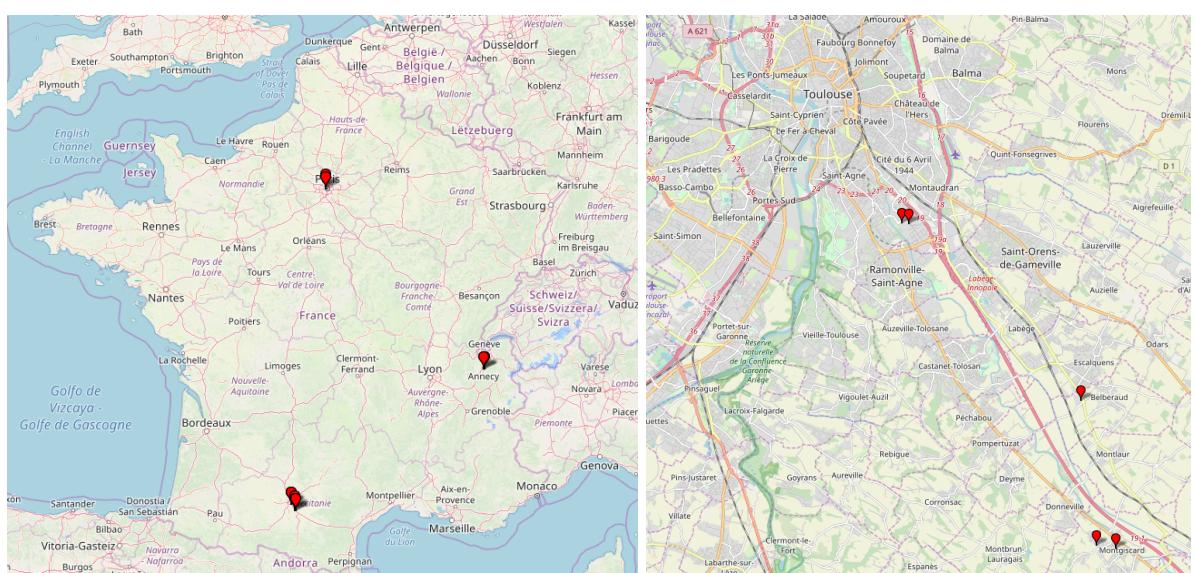


FIGURE 2.3 – Zones d'intérêt de l'utilisateur 1 pour un temps où l'immobilité est considérée à 5 minutes, pour une distance de 100m

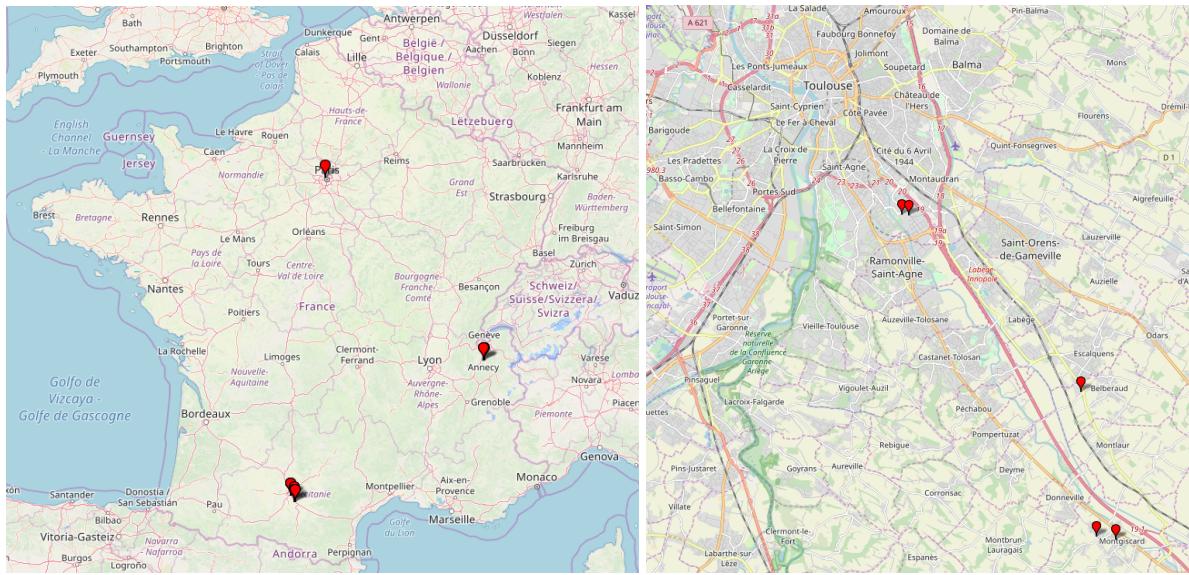


FIGURE 2.4 – Zones d'intérêt de l'utilisateur 1 pour un temps où l'immobilité est considérée à 5 minutes, pour une distance de 50m

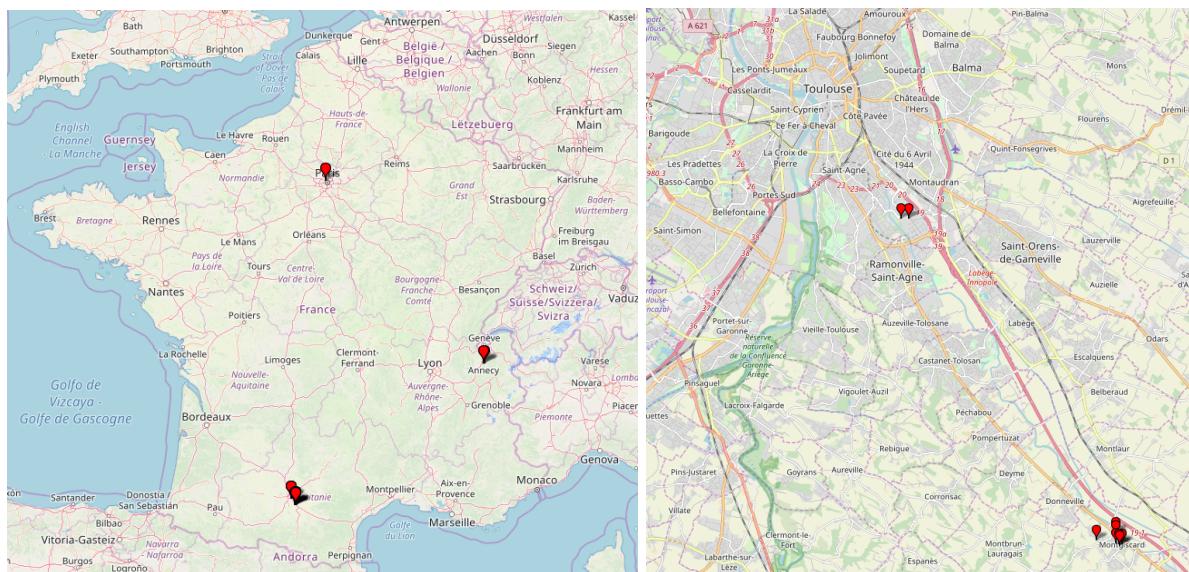


FIGURE 2.5 – Zones d'intérêt de l'utilisateur 1 pour un temps où l'immobilité est considérée à 5 minutes, pour une distance de 10m

Le bon réglage de la résolution spatiale est crucial, car deux phénomènes opposés sont à l'oeuvre, et conditionnent l'apparition de clusters, comme illustré sur les images ci-dessus. En effet, pour une résolution souple (e.g. 1km), nous assurons d'avoir un certain nombre de clusters, car il est probable que l'individu se retrouve fréquemment dans des situations d'immobilité à cette échelle. En revanche, nous risquons de fusionner plusieurs points intéressants, en particulier à l'échelle du quartier. Nous constatons qu'à résolution souple, nous n'avons qu'un seul point pour le quartier de résidence de l'individu, qui se transforme en une multitude de points d'intérêts pour une résolution plus exigeante. Nous pouvons imaginer que ces points correspondent à l'école des enfants, ou les commerces locaux par exemple. Il est donc nécessaire de renforcer la résolution spatiale pour obtenir des résultats plus précis.

Il n'est toutefois pas souhaitable d'être trop exigeant sur ce critère, car certains points d'intérêts ne seraient pas identifiés comme cluster, car l'activité qui y est réalisée n'est pas complètement immobile. L'exemple le plus clair est celui du centre commercial Super U de Belberaud : l'individu s'y déplace durant ses courses, nous pouvons donc l'identifier comme cluster pour une résolution de l'ordre de la taille du centre commercial ou plus large, mais pas pour une résolution trop exigeante comme 10m par exemple.

2.2 Attaque BE de l'utilisateur 2

Les comparaisons pour différentes résolutions spatiale et temporelle ont déjà été effectuées pour l'individu 1, nous avons donc désormais choisi les paramètres que nous jugeons optimaux (1km et 10 min), et présentons les résultats de l'attaque uniquement avec ces paramètres.

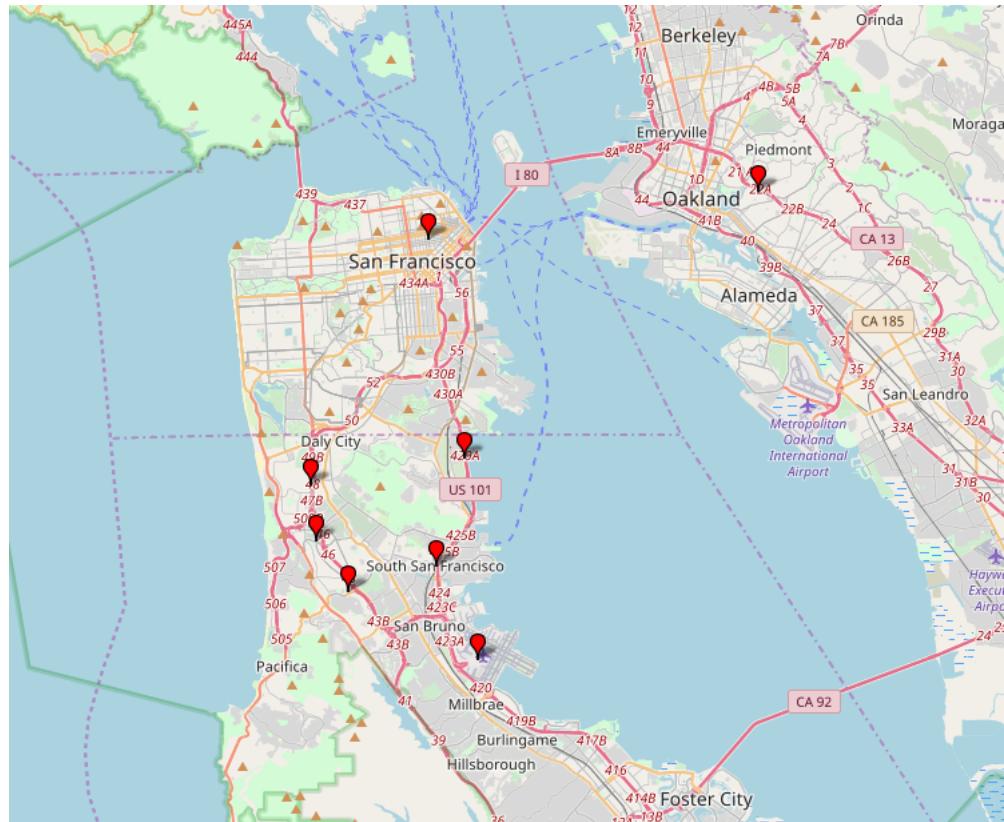


FIGURE 2.6 – Zones d'intérêt de l'utilisateur 2 pour un temps où l'immobilité est considérée à 10 minutes, pour une distance de 1 km

Nous déduisons de cette attaque que l'individu travaille principalement dans le centre de San Francisco. Nous observons un point au niveau de l'aéroport. Nous en déduisons que le taxi récupère de nombreux clients à l'aéroport international de San Francisco pour par la suite les amener en centre ville. L'aéroport est un endroit où le taxi attend relativement longtemps sans se déplacer car il doit faire la queue pour récupérer des clients.

2.3 Attaque BE de l'utilisateur 3

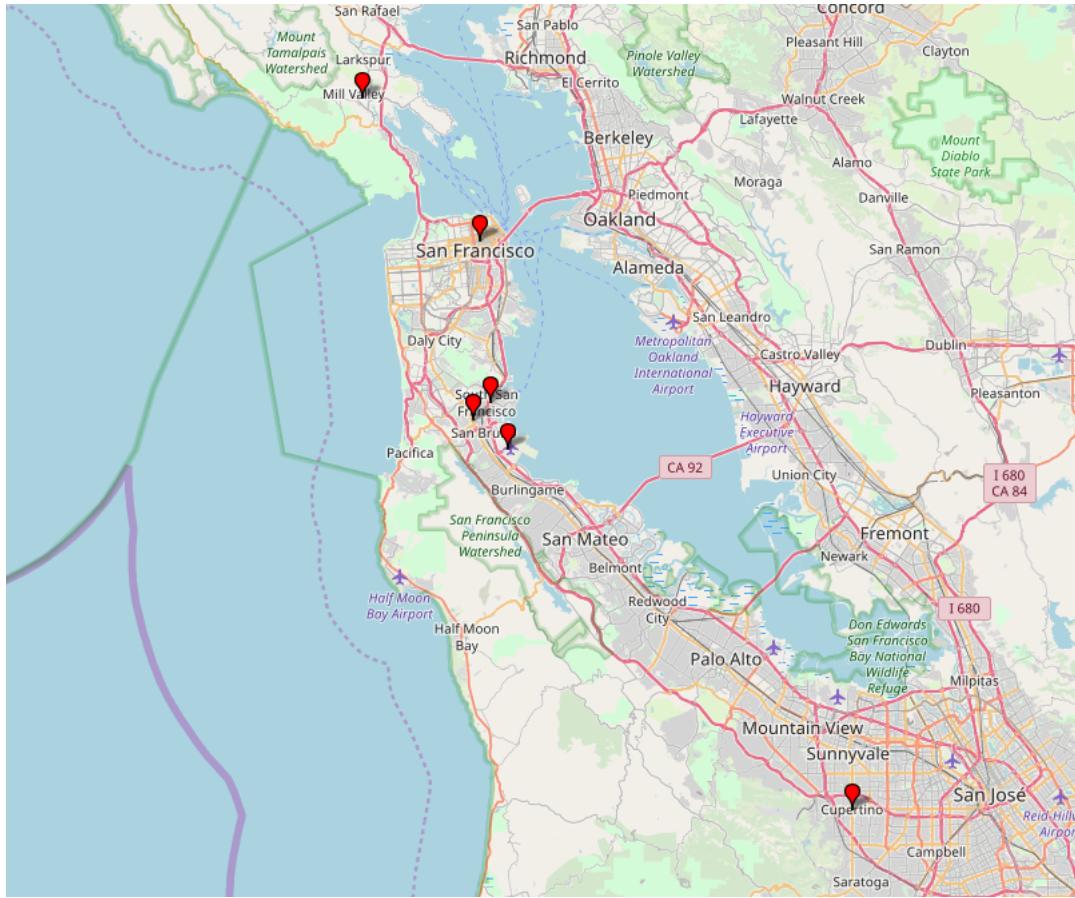


FIGURE 2.7 – Zones d'intérêt de l'utilisateur 3 pour un temps où l'immobilité est considérée à 5 minutes, pour une distance de 1 km

Nous pouvons voir que comme l'utilisateur 2, ce taxi présente un cluster au niveau de l'aéroport international. Cependant, son périmètre d'action semble plus important. En effet, alors que l'utilisateur 2 avait tous ses clusters localisés en centre-ville de San-Francisco, l'utilisateur 3 semble présenter des clusters localisés tout autour de la baie de San Francisco.

3 Attaque k-means

3.1 Attaque k-means de l'utilisateur 1

Dans le cadre de cette attaque, nous avons implémenté sous Python un algorithme de k-means sur les positions de l'individu. Cette fois-ci, l'immobilité n'est pas prise en compte, mais plutôt la fréquence des positions autour d'une moyenne locale. Nous avons donc ici un seul paramètre sur lequel jouer : le "k", c'est à dire le nombre de clusters souhaités. Pour l'individu 1, nous trouvons les points d'intérêt suivants selon les valeurs de k :

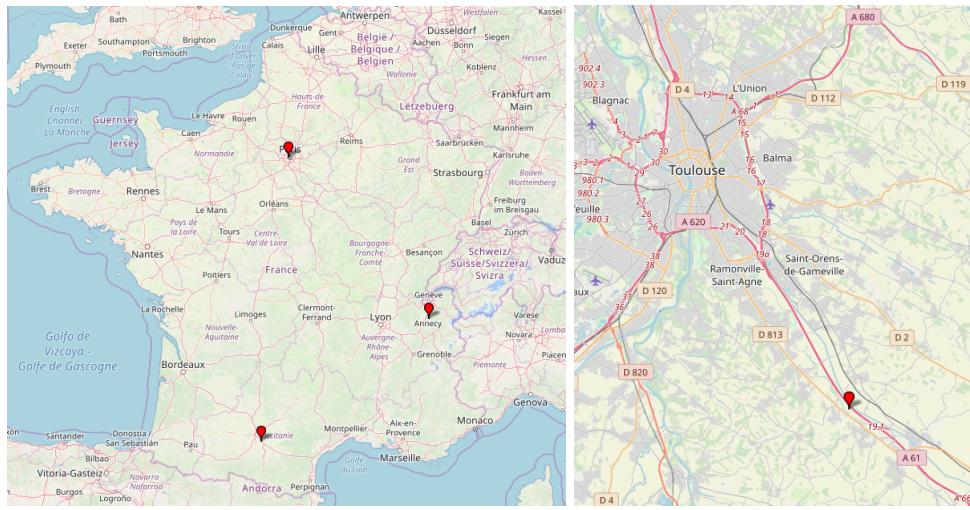


FIGURE 3.1 – Attaque 3-means sur l'utilisateur 1

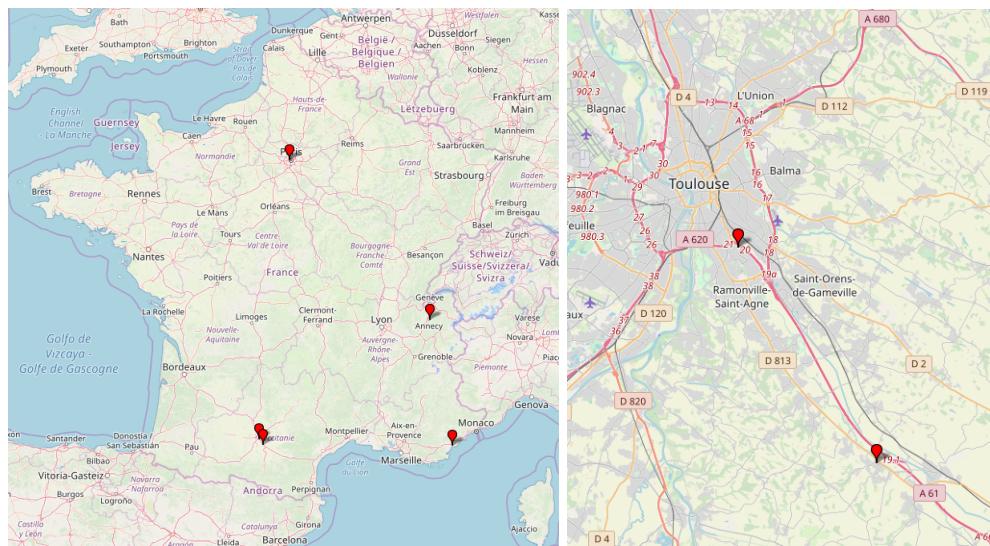


FIGURE 3.2 – Attaque 5-means sur l'utilisateur 1

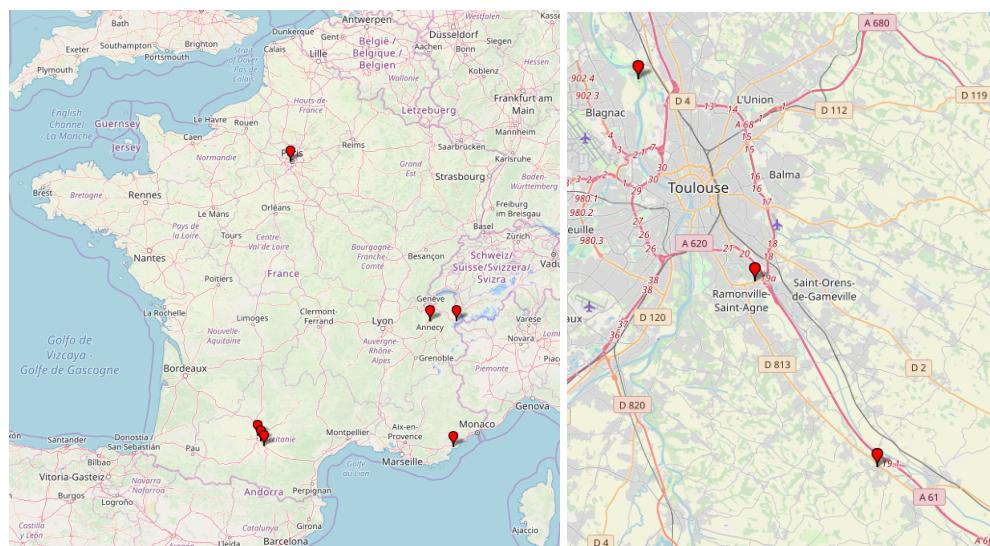


FIGURE 3.3 – Attaque 7-means sur l'utilisateur 1

Nous constatons que la distance est très fortement pondérée lors de la création des k groupes, les premiers groupes formés sont donc les villes visitées au cours de la période considérées. Il est donc nécessaire de choisir k plus grand que ce nombre de villes visitées, car c'est seulement une fois ce nombre franchi que nous pourrons observer des points d'intérêts différents à l'intérieur de la ville, notamment de Toulouse dans ce cas.

Nous observons que pour l'individu 1, l'attaque k-means donne des résultats différents, voire moins bons, que l'attaque précédente. Cette méthode est plus adaptée à reconnaître des grands déplacements, tels que des vacances. On remarque notamment des déplacements à Annecy ou encore Saint-Raphaël. Néanmoins, nous avions déjà récolté ces informations par l'attaque BE. Nous avons perdu certaines informations, notamment le centre commercial de Belberaud, ou les points d'intérêts à l'intérieur du quartier, car ces points sont trop proches, et nécessiteraient donc un grand k, ce qui noiera l'information.

3.2 Attaque k-means de l'utilisateur 2

Nous savons que les déplacements des deux utilisateurs 2 et 3 sont contenus dans la région de San Francisco, nous n'aurons donc cette fois pas besoin d'un k trop grand, car il n'y a pas de trop grande variation de distance. Le preprocessing de ces deux individus est ici vraiment intéressant, car les distances des points erronés auraient nécessairement impliqué des clusters à ces endroits.

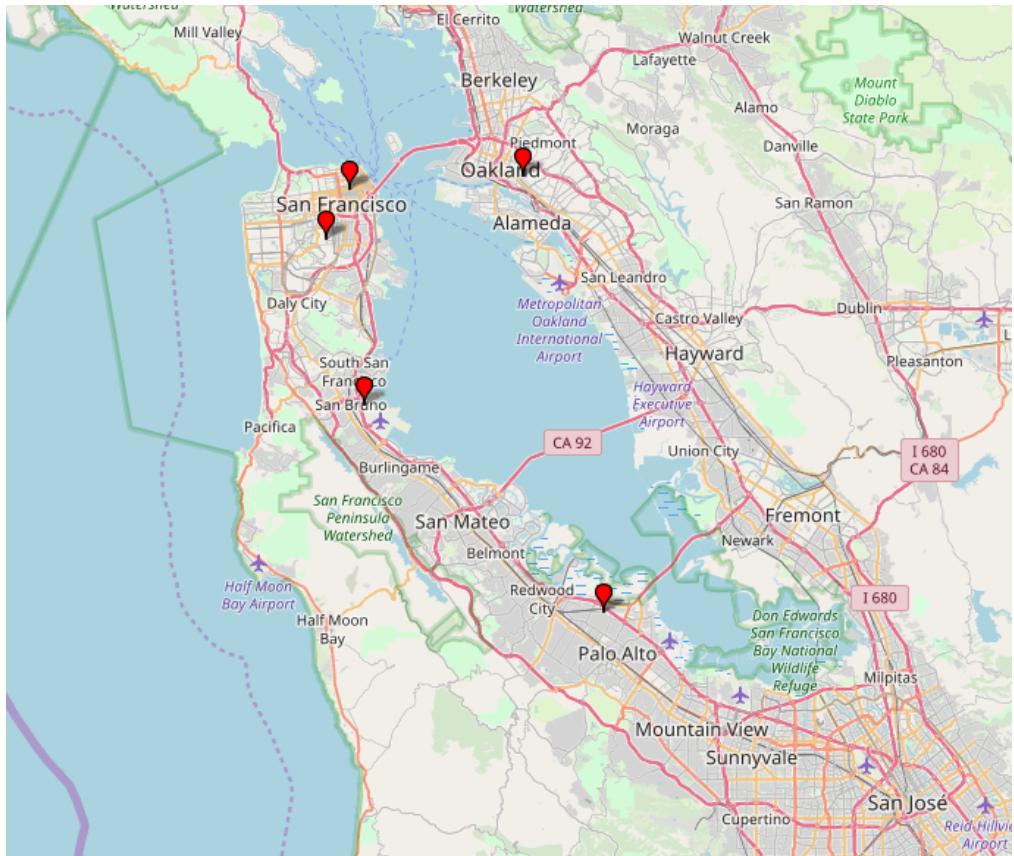


FIGURE 3.4 – Attaque 5-means sur l'utilisateur 2

Alors qu'elle n'était pas particulièrement adaptée au cas de l'individu 1, nous constatons ici que la méthode k-means donne des résultats plus exploitables que précédemment. Cela paraît logique, car un chauffeur de taxi peut facilement se retrouver à attendre 10 min au domicile d'un client, créant un point inutile, alors que prendre en compte la fréquence des points est plus adapté compte tenu de son métier.

Les courses exceptionnellement lointaines apparaissent (notamment celle vers Palo Alto), délimitant le périmètre d'action de ce chauffeur. Nous retrouvons à nouveau un point dans le centre de San Francisco, ce qui semble être le domicile de cet individu.

3.3 Attaque k-means de l'utilisateur 3

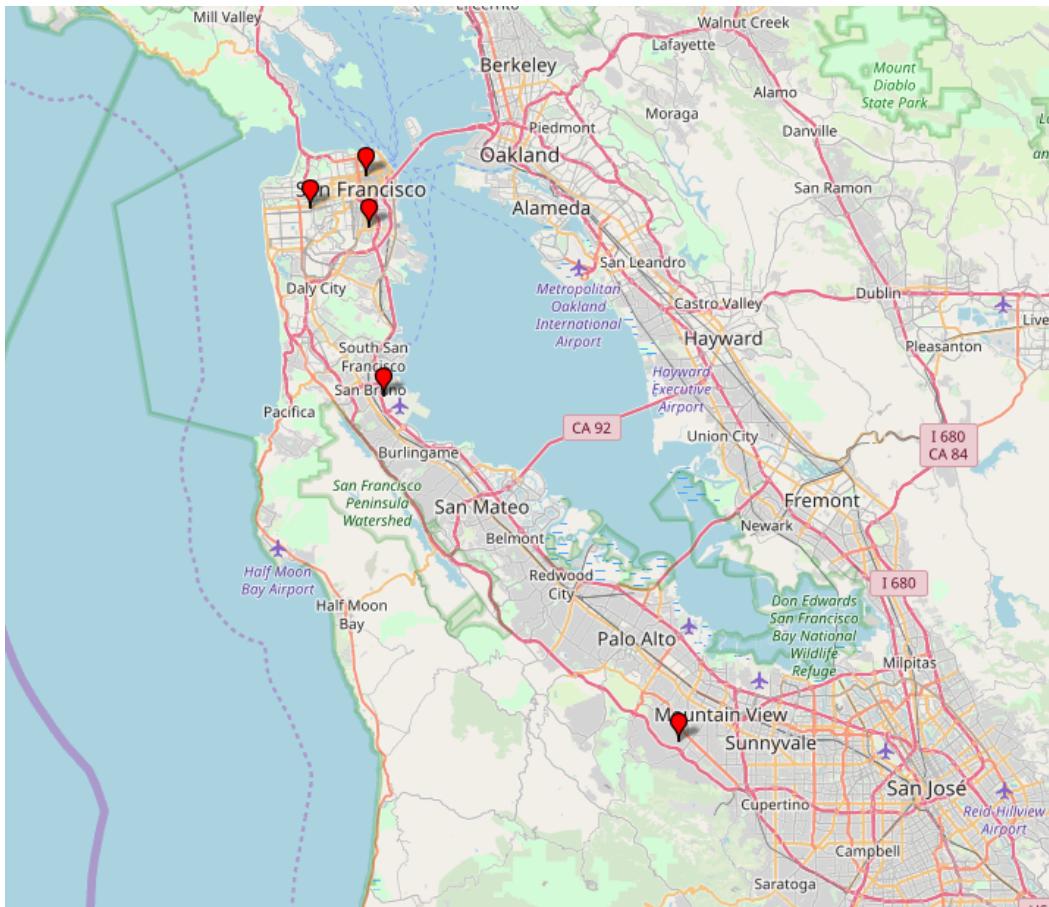


FIGURE 3.5 – Attaque 5-means sur l'utilisateur 3

Nous pouvons appliquer les mêmes remarques sur cette attaque que lors de l'attaque de l'utilisateur 2. L'utilisateur 3 présente encore un point localisé près de l'aéroport confirmant nos hypothèses sur le fait qu'il cherche beaucoup de ses clients à l'aéroport. On retrouve également la présence de cluster en plein centre de San Francisco, nous montrant que la majorité de ses courses mène ou provient du centre ville de San Francisco.