REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
UNIVERSITE MOHAMED KHIDER DE BISKRA

Faculté des sciences exactes et sciences de la nature et de la vie

Département d'Informatique

N° d'ordre :. . . . . .
Série :. . . . . .

T H È S E
Présentée en vue de l'obtention du diplôme de
Doctorat en Science en Informatique

Spécialité : **INFORMATIQUE**

Titre de la Thèse :

Une approche de sécurité pour le M-Business

Par : **Aloui Ahmed**
Le : / /

Devant le jury composé de :

Laskri Mohamed Tayeb	**Président**	**Professeur à Université d'Annaba.**
Kazar Okba	**Rapporteur**	**Professeur à Université de Biskra.**
Kimour Mohamed Taher	**Examinateur**	**Professeur à Université d'Annaba.**
Bennoui Hammadi	**Examinateur**	**Professeur à Université de Biskra.**
Jean-Marc Petit	**Examinateur**	**Professeur à INSA de Lyon, France.**
Ayad Soheyb	**Examinateur**	**MCA à Université de Biskra.**

Remerciements

Tout d'abord, Mes louanges à **DIEU** le Tout Puissant pour m'avoir donné le courage, la volonté, la patience durant ces années d'étude et que grâce à Lui ce travail a été réalisé.

Les travaux de recherche dans le cadre de cette thèse sont effectués au sein du Laboratoire de l'INFormatique Intelligente Biskra (L I N F I) de l'université Mohamed Khider sous La direction de Mr **Okba KAZAR** Professeur à l'université Mohamed Khider de Biskra. Qu'il trouve ici le témoignage de ma profonde gratitude et mes sincères remerciements. Ses qualités scientifiques et humaines ont Toujours été une source de motivation. Son aide et ses conseils m'ont été toujours précieux.

Je remercie très vivement Mr **Laskri Mohamed Tayeb Professeur** Professeur à l'université d'Annaba pour l'honneur qu'il me fait en acceptant de présider le jury.

Mes vifs remerciement vont également aux honorables membres de jury : Mr **Kimour Mohamed Taher** Professeur à l'université d'Annaba, Mr **Bennoui Hammadi** Professeur à l'université Mohamed Khider de Biskra, Mr **Jean-Marc Petit** Professeur à l'université de Lyon, Mr **Ayad Soheyb** Maître de conférences à l'université de Biskra.

Enfin je tiens à remercier tous ceux et celles qui m'ont aidé et soutenu de près ou de loin pour l'accomplissement de cette thèse.

Ahmed Aloui

Dédicaces

Je dédie ce modeste travail :

À ceux que j'ai de plus cher au monde, mes parents. Et je remercie infiniment mes parents pour leur support continu, ce qui a renforcé ma motivation et me mène à achever mon doctorat dans les meilleures conditions.

À mes frères et soeurs, ainsi qu'à tous mes amis.

Un remerciement particulier à mon épouse et mes enfants (Aymen et Fatma) pour leur patience à mon indisponibilité permanente durant la préparation de cette thèse.

Ahmed Aloui

Abstract

Privacy-preserving in mobile business supplying location-based services (LBS) has the potential to become a primary concern for clients and service providers (LPs). In m-business providing LBS services, a client sends its exact locations to service providers. This data may involve sensitive and private personal information. Therefore, the misuse of location information by service providers creates privacy issues for clients. Moreover, the query must not be linked to the mobile client, even if the location information is exposed willingly by her/him to obtain specific services. Thus, there are location cloaking approaches that allow the protection of the location privacy of mobile users. Hence, many temporal and spatial approaches to cloaking a specific user's location have been proposed. Different from existing approaches, in this thesis, we investigate issues related to the mobile client' privacy (i.e. the location privacy and the query privacy in the same cloaking process). Particularly, we aim to preserve the client location privacy as well as the continuous queries privacy, where mobile clients continuously emit different queries during their travels. It's on this premise that we propose a new clique-based cloaking approach named Mobile Clique Cloak (MCC) to preserve the mobile client's privacy in the M-business providing LBS services. Also, to build the cloaking region in our approach, we take into account the similarity of clients velocity, acceleration and direction to obtain a good balance between quality of service QoS and privacy. Moreover, our work deals with a series of attacks in the same cloaking process (location attack, tracking attack, query sampling attacks and homogenous attack). We evaluate our approach from three aspects : privacy guaranty, quality of service and performance. Experimental evaluation of our approach on a real world map shows that our approach ensures total privacy for clients and protects the privacy of clients during the entire query period whiles allowing clients' choice of privacy requirements. Besides, we compare our approach with existing privacy protection approaches such as V-DCA, D-TC and GCA. According to the evaluation results and a comparison of the approaches, our approach MCC can make a good balance between quality of service, performance and privacy.

Keywords : *Mobile business (m-business), Security, Privacy preservation, Location-based services (LBS), Mobility, Client privacy protection, Location and query privacy, Snapshot query, Continuous query, K-anonymity, Cloaking, Clique, Quality of service (QoS), Dummy and Similarity of movement.*

Résumé

La protection de la vie privée dans le business mobile (m-business) fournissant des services basés sur la localisation (LBS) peut devenir une préoccupation majeure pour les clients et les fournisseurs de services. Dans m-business, un client envoie ses emplacements exacts aux fournisseurs de services (LPs). Ces données peuvent impliquer des informations personnelles sensibles et privées. Par conséquent, l'utilisation abusive des informations de localisation par les fournisseurs de services crée des problèmes de la vie privée pour les clients. De plus, la requête ne doit pas être liée au client mobile, même si les informations de localisation sont volontairement exposées par lui (client mobile) pour obtenir certains services. Pour cela, il existe des approches de camouflage (masquage) qui permettent de protéger la vie privée de l'emplacement des clients mobiles. Par conséquent, de nombreuses approches temporelles et spatiales ont proposé pour masquer l'emplacement d'un utilisateur spécifique (par exemple, k-anonymity, l-Diversity). Les travaux actuels définissent la vie privée de l'emplacement et la vie privée de requête séparément. Ainsi, dans le contexte de cette thèse, nous étudions les problèmes liés à la vie privée du client mobile. En particulier, nous visons à préserver la vie privée de l'emplacement du client ainsi que la vie privée des requêtes continues, où différentes requêtes sont émises en continu par les clients mobiles au cours de leurs déplacements. C'est sur cette prémisse que nous proposons une nouvelle approche basée sur une clique nommée MCC pour préserver la vie privée du client mobile dans le m-business fournissant des services LBS. De plus, afin de construire la région de camouflage dans notre approche, nous considérons la similitude de la vitesse, de l'accélération et de la direction des clients pour obtenir un bon équilibre entre la qualité de service (QoS) et la vie privée. De plus, notre travail porte sur une série d'attaques dans le même processus de protection (attaque de localisation, attaque de suivi, attaques par échantillonnage de requêtes et attaque homogène). Nous évaluons notre approche sous trois aspects : garantie de la vie privée, qualité de service et performance. Une évaluation expérimentale de notre approche sur une carte du monde réel montre que notre approche garantit la vie privée totale pour les clients et protège la vie privée des clients pendant toute la période de requête tout en permettant aux clients de choisir les exigences de la vie privée. En outre, nous comparons notre approche avec des approches de protection de la vie privée existants tels que V-DCA, D-TC et GCA. Selon les résultats de l'évaluation et après la comparaison avec quelques approches existantes, nous concluons que notre approche peut faire un bon équilibre entre qualité de service, performances et la vie privée.

Mots clés : *business mobile (m-business), Sécurité, Préservation de la vie privée, Les services de localisation (LBS), Mobilité,Protection de la vie privée des clients, Vie privée de l'emplacement, Vie privée des requêtes, Requête continue, K-anonymat, Cloaking, Clique, Qualité de service (QoS), Dummy et Similarité du mouvement.*

ملخص:

يمكن أن تصبح الخصوصية في الأعمال المتنقلة التي تقدم خدمات تعتمد على الموقع مصدر قلق كبير للعملاء ومقدمي الخدمات. في الأعمال المتنقلة، يرسل العميل مواقعه بالضبط إلى مزودي الخدمة. قد تتضمن هذه البيانات معلومات شخصية حساسة وخاصة. لذلك، يؤدي سوء استخدام معلومات الموقع من قِبل موفري الخدمة إلى إنشاء مشكلات خصوصية للعملاء. بالإضافة إلى ذلك، يجب ألا يكون الطلب مرتبطًا بعميل الهاتف المحمول، حتى إذا كانت معلومات الموقع مكشوفة من قِبله للحصول على خدمات معينة. لهذا، هناك خوارزميات تمويه الموقع (حماية) التي تحمي خصوصية موقع عملاء الأجهزة المحمولة. لذلك، تم اقتراح العديد من الأساليب الزمانية والمكانية لإخفاء موقع مستخدم معين. تعمل الأعمال الحالية على تحديد خصوصية الموقع وخصوصية الاستعلام بشكل منفصل.

وبالتالي، في سياق هذه الرسالة، ندرس المشاكل المتعلقة بخصوصية العميل. على وجه الخصوص، نحن نهدف إلى الحفاظ على خصوصية موقع العميل وكذلك خصوصية الطلبات المستمرة، حيث يتم تقديم طلبات مختلفة بشكل مستمر من قبل عملاء الجوال أثناء التنقل. بناءً على هذه الفرضية، نقترح خوارزمية إخفاء جديدة تستند إلى نقرة تسمى "(MCC)" للحفاظ على خصوصية العميل في الأعمال التجارية المتنقلة التي توفر خدمات LBS. بالإضافة إلى ذلك، من أجل بناء منطقة التمويه في النهج الذي نتبعه، نأخذ في الاعتبار تشابه سرعة العملاء وتسارعهم واتجاههم للحصول على توازن جيد بين جودة الخدمة والخصوصية. بالإضافة إلى ذلك، يركز عملنا على سلسلة من الهجمات في نفس عملية الحماية. نقوم بتقييم نهجنا في ثلاثة جوانب: ضمان الخصوصية وجودة الخدمة والأداء. يوضح التقييم التجريبي لخوارزمياتنا على خريطة العالم الحقيقي أن نهجنا يضمن الخصوصية الكاملة للعملاء ويحمي خصوصية العميل طوال فترة الطلب مع السماح للعملاء باختيار متطلبات الخصوصية. بالإضافة إلى ذلك، نقوم بمقارنة خوارزمياتنا بخوارزميات الخصوصية الحالية مثل V-DCA و D-TC و GCA. اعتمادًا على نتائج التقييم ومقارنة الخوارزميات، وجادنا أن الحل المقترح يحقق توازنًا جيدًا بين جودة الخدمة والأداء والخصوصية.

الكلمات المفتاحية: الأعمال المتنقلة، الأمن، الحفاظ على الخصوصية، خدمات الموقع، التنقل، حماية خصوصية العملاء، خصوصية الموقع، خصوصية الطلبات، طلب مستمر، جودة الخدمة وتشابه الحركة.

Table des matières

Table des figures

Liste des tableaux

Chapitre 1

Introduction Générale

1.1 Contexte

Le business mobile (m-business) désigne les activités de business électronique effectuées à l'aide d'appareils portables tels que des téléphones cellulaires et des assistants numériques personnels (Personal Digital Assistant PDA) via Internet mobile. Le m-business présente de nouvelles caractéristiques (fonctionnalités) telles que la mobilité, l'instantanéité, la personnalisation et la commodité, par rapport au business électronique classique. Les deux caractéristiques principales de m-business sont la mobilité et la commodité pour les utilisateurs. Parce que la mobilité et la commodité rendent les utilisateurs se sentent libres. Grâce à m-business, les utilisateurs seront totalement mobiles, ils peuvent également contrôler leurs affaires de n'importe où (par exemple, à la maison, dans les transports ainsi que dans plusieurs lieux de travail). De plus, avec l'e-business, les gens peuvent être limités aux stations de bureau.

Par ailleur, les utilisateurs à l'aide d'appareils mobiles peuvent accéder aux services basés sur la localisation (Location Based Services LBS). LBS est une classe générale de services d'information accessibles à l'aide d'informations sur les localisations géographiques d'appareils mobiles basées sur des technologies de communication mobile telles que le système de positionnement global (GPS) et réseaux cellulaires. Ces dernières années, avec l'application généralisée des nouvelles technologies de l'information et de la communication, le m-business a connu une croissance rapide. Par conséquent, de nouveaux types d'applications de m-business fournissant des LBS sont devenus populaires. En plus, LBS est une composante fondamentale de m-business pour améliorer la qualité des services (QoS). Ainsi que le rôle le plus important de LBS est la fourniture des informations personnalisées à l'utilisateur mobile en fonction du contexte de l'emplacement de l'utilisateur.

Les services de LBS accueillent chaque jour des millions d'utilisateurs. De plus, leur utilité oblige en quelque sorte les utilisateurs à révéler leurs coordonnées géographiques. En outre, les données de géolocalisation représentent l'information de base

dans le m-business, et représentent en même temps l'entité qui pose le plus de risques de violation de la vie privée. Dans la plupart des pays, les coordonnées géographiques ne peuvent pas être collectées sans fournir aux utilisateurs des garanties de confidentialité conformément à la législation de protection des données. Cependant, les règles de confidentialité ne peuvent pas protéger les informations personnelles contre les parties malveillantes essayant d'accéder à ces données sans le consentement de l'utilisateur.

La publicité ciblée, le marketing et le profilage sont devenus des outils largement utilisés dans l'économie actuelle. Pour cela, les informations de l'emplacement collecté constituent une source utile et précieuse pour les entreprises. De plus, les utilisateurs ignorent souvent la vie privée et décident souvent de divulguer ou non ces informations immédiatement. Selon [5] les revenus du marché de m-business basés sur la localisation ont augmenté de 10,3 milliards d'euros en 2014 et devraient atteindre à 34,8 milliards d'euros en 2022. Cependant, selon une enquête effectuée par Microsoft en 2011, la principale raison pour laquelle les gens ne voulaient pas adopter le m-business basés sur la localisation était la préoccupation de la vie privée personnelle de l'utilisateur (par exemple, les problèmes de la vie privée liés à l'emplacement de l'utilisateur, Location Privacy).

1.2 Problématique

Cette thèse se concentre sur deux aspects principaux liés à l'utilisation des services de m-business. Le premier aspect est la protection de la vie privée des utilisateurs de m-business qui considèrent les fournisseurs de services comme un adversaire à qui les utilisateurs ne devant en aucun cas fournir leurs coordonnées géographiques. Le deuxième aspect est de garantir de l'utilité de service. Il s'agit de conserver tous les avantages du fournisseur de services tout en respectant la vie privée des utilisateurs. Par conséquent, il s'agit de trouver la meilleure façon de révéler ce qu'il faut pour obtenir les résultats souhaités. Avec le développement rapide les technologies mobile et les technologies de détection de la localisation, telles que le système de positionnement global (GPS) et les réseaux cellulaires, le business mobile est devenu omniprésent. La géolocalisation ajoute la dimension qui permet au service du m-business d'associer toute action, interaction ou tout événement commis en ligne à des coordonnées géographiques. Par exemple, le cas du business géo-dépendant, ou un client reçoit des offres commerciales en fonction de son emplacement actuel, représente la forte relation qui a émergé du développement de LBS.

Dans le m-business, pour obtenir un service, l'utilisateur envoie des requêtes qui contiennent leur emplacement exact aux fournisseurs de services. Ce type d'information est très utile et ces données peuvent impliquer des informations personnelles sensibles et privées. En conséquence, les fournisseurs de services peuvent utiliser abusivement les informations de localisation de l'utilisateur, ce qui crée des problèmes de vie privée pour

les utilisateurs. Étant donné de la sensibilité de ce type d'information, les utilisateurs voudront savoir que leurs informations sont entre de bonnes mains avant d'envisager l'adoption des services de m-business.

Il existe des requêtes instantanées (Snapshot queries) et des requêtes continues (Continuous queries). Pour le cas de requête instantanée, le client envoie ses données de localisation une fois, reçoit les résultats de la requête du fournisseur de services, puis termine la requête, par exemple «Récupérer tous les hôtels autour de moi dans un cercle de 2 km de rayon». Pour les requêtes continues, le client envoie l'emplacement périodiquement pour recevoir une version mise à jour des résultats de la requête (par exemple, tous les 20 s).

Les fournisseurs de services peuvent collecter, traiter et stocker les emplacements des utilisateurs mobiles. En outre, les fournisseurs de services sont souvent capables de suivre ou d'enregistrer les mouvements de leurs utilisateurs avec une grande précision spatiale et temporelle. En conséquence, ils peuvent générer un historique complet des mouvements de chaque utilisateur, y compris le type de services basés sur la localisation auxquels ils ont accédé et le moment de l'accès. Cependant, il est clair que les informations personnelles de ce type ont une valeur commerciale. Il existe également des entreprises qui conservent les informations aussi longtemps que possible pour une exploitation commerciale future de ces informations. Par conséquent, l'analyse des données de localisations collectées et la mauvaise d'utilisation de ces informations, que ce soit accidentelle ou volontaire, par les fournisseurs non fiables (indigne de confiance) créant des problèmes de sécurité. Autrement dit, la vie privée d'un client peuvent être divulguées aux des tierces parties.

Dans le m-business, il existe trois types d'informations doivent être protégé : l'emplacement et l'identité du client mobile (Id), ainsi que le contenue de la requête sensible. En outre, les utilisateurs mobiles ne veulent pas révéler leurs emplacements et/ou leurs requêtes aux fournisseurs de services. Parce que, les informations de localisation peuvent révéler des informations sensibles sur les utilisateurs mobiles, telles que les affiliations politiques, religieuses, les adresses de domicile et de travail, les activités quotidiennes, la situation financière, les problèmes de santé d'une personne (si, par exemple, l'emplacement de la requête est l'hôpital).

En plus, la connaissance de l'emplacement peut aussi mener au traquer (suivis) des utilisateurs. Par conséquent, la préservation de la vie privée de la localisation est essentielle pour le déploiement réussi de m-business. En général, les approches de protection de la vie privée sont utilisées pour fournir une divulgation partielle des données de l'utilisateur. Dans le contexte de m-business fournissant LBS, la divulgation partielle des informations de l'emplacement de l'utilisateur est nécessaire pour fournir le service à l'utilisateur mobile avec un niveau de Qos accepté.

En réalité, le niveau de Qos requis varie selon la nature de chaque service de m-business. Par conséquent, afin d'atteindre le niveau de qualité exigé par l'utilisateur,

il est indispensable pour les utilisateurs d'avoir la possibilité d'ajuster le niveau de la vie privée de l'emplacement pour chaque service. Attendu que, la QoS se dégrade fortement si l'emplacement de service signalé est à plusieurs centaines de mètres de l'emplacement réel de l'utilisateur mobile.

Comme nous l'avons vu précédemment, l'utilisation de m-business soulève de graves préoccupations concernant la protection de la vie privée des utilisateurs mobiles. La protection de la vie privée des utilisateurs est donc un problème de sécurité important pour le déploiement le m-business [6]. Pour cela, une approche de protection de la vie privée des utilisateurs mobile est extrêmement importante.

Dans notre thèse, nous allons étudier cette problématique en essayant de répondre à des questions suivantes : Comment peut-on protéger l'emplacement exact du client ?, et en même temps, comment peut-on empêcher l'adversaire de lier les requêtes à un client particulier ? Comment peut-on obtenir un bon équilibre entre QoS et la protection de la vie privée ?

1.3 Motivation techniques

Généralement, les techniques de la protection de la vie privée des utilisateurs ont des structures différentes selon les informations protégées et le modèle d'attaque. Ces techniques incluses : Obfuscation / Cloaking spatiale, k-anonymat, Dummies, les zones mix, et le cryptage. En plus, le but de ces techniques est de brouiller ou de réduire la résolution de l'emplacement de l'utilisateur envoyé efficacement au fournisseur de service. En d'autres termes, ces techniques visent à faire le compromis entre la vie privée de l'utilisateur et l'utilitaire de service avec un niveau acceptable de calcul et les frais généraux de communication. La technique de Cloaking spatiale basée sur k-anonymat est massivement utilisée pour la protection de la vie privée de la localisation, ainsi que pour la vie privée des requêtes. Le Cloaking spatiale peut utiliser pour satisfaire des exigences spécifiques de la vie privée en brouillant les emplacements exacts des utilisateurs dans des régions masquées (une région de cloaking) [7] et [8].

Cette technique est habituellement intégrée dans des applications dans différents environnements afin de réduire au minimum la divulgation des informations personnelles lorsque les utilisateurs demandent un service de m-business. Étant donné que le fournisseur de services ne reçoit pas les informations de localisation exactes, un ensemble comprenant la solution satisfaisante serait renvoyé à l'utilisateur. Les exigences générales de la vie privée comprennent le K-anonymat, la superficie maximale et la superficie minimale [7]. Pour s'assurer que les attaquants ne peuvent être récupérés que des informations à gros grains lors de la réception d'une demande de l'utilisateur, les approches de cloaking visent à réduire l'exactitude de l'emplacement du l'utilisateur en étendant l'emplacement exact du l'utilisateur dans une région de cloaking qui contient non seulement l'emplacement de l'utilisateur, mais aussi au moins k-1 autres

utilisateurs.

1.4 Contributions

Pour la protection de la vie privée de l'utilisateur dans le m-business, il existe trois types d'architectures : client-serveur, tiers de confiance, et l'architecture basé sur les pairs. Dans notre travail, nous adoptons l'architecture de tiers de confiance (Trusted Third Party TTP) composée d'utilisateurs mobiles, un serveur d'anonymisation (**AS**) et les fournisseurs de services. Le modèle TTP utilise le concept de middleware entre l'utilisateur mobile et le fournisseur de services. Nous désignons le middleware en tant que serveur d'anonymisation (**AS**). Les requêtes de l'utilisateur mobile sont envoyées à l'AS, la requête est alors masquée dans une région avec une tolérance spatiale et temporelle. Nous appelons cela *requête de la région.*

Dans cette thèse nous avons proposé une approche de sécurité basée sur le cloaking pour la protection de la vie privée des utilisateurs dans le m-business, mais diffère de [9], [10], [11] et [12] dans plusieurs aspects. Tout d'abord, les approches de cloaking dans [9] et [10] concernent la protection de la vie privée de l'emplacement seulement ; alors que l'objectif de notre approche est de protéger la vie privée de l'emplacement et la vie privée de la requête aussi. En plus, l'approche dans [9] concerne la protection de la vie privée pour les requêtes d'instantané et peut donc souffrir d'attaques requêtes continues, alors que notre approche concerne la protection de la vie privée pour les requêtes continues. Deuxièmement, dans [10] les auteurs ont proposé une approche de protection de la vie privée mais ils n'ont pas pris en considération les mouvements des utilisateurs mobiles. Par conséquent, pour construire une région de cloaking dans notre approche, nous prenons en considération la similarité des mouvements des utilisateurs mobiles comme les caractéristiques de la vitesse, l'accélération et la direction. Les résultats d'analyse montrent que notre approche peut obtenir un bon équilibre entre QoS et la vie privée.

En plus, les techniques actuelles de l'anonymisation centrale (TTP) comme [9], [13], [14] et [15] seront sous-performances, puisque si les k-1 autres utilisateurs ne sont pas disponibles au moment de la requête de l'utilisateur mobile alors cette requête est rejeté. Dans ce cas, le système peut être évalué comme peu fiable.

Contrairement aux travaux précédents, dans notre approche, toutes les requêtes seront traitées même si k-1 d'autres utilisateurs ne peuvent pas être trouvés. Pour ce faire, nous produisons des différents Dummies au lieu de rejeter la requête. La différence entre notre travail et le travail de [12] est que les Dummies générés doivent prendre les mêmes caractéristiques des similarités de mouvement de l'utilisateur (l'émetteur de requête).

Une attaque contre la vie privée est une attaque qui se produit lorsqu'une entité malveillante tente d'obtenir l'identité de l'utilisateur et ses informations personnelles

pour suivre les activités et les mouvements de l'utilisateur. En outre, dans les travaux précédents, les auteurs ne fournissent pas approche générale prenant en compte tous les types d'attaques contre la vie privée des utilisateurs. Autrement dit, chaque approche de protection contre un seul type d'attaque spécifique. Par conséquent, nous avons proposé une approche de protection prenant en compte une série d'attaques contre la vie privée des utilisateurs dans le même processus de protection (location attack, tracking attack, linking attack, query sampling attacks and homogeneity attack). Comme particularité de notre contribustion, elle traite une série d'attaques dans le même processus de protection.

Pour répondre aux questions précédemment posées, notre thèse apporte les principales contributions suivantes :

- ✓ Proposition un nouvel algorithme de préservation de la vie privée de l'utilisateur mobile nommé MCC (Mobile Clique Cloak) pour les requêtes continues dans m-business fournissant des LBS. En outre, nous prenons en compte la similarité de mouvement des utilisateurs mobiles (la vitesse, la direction et l'accélération) lors de la génération des régions de cloaking.
- ✓ En plus, nous avons traité les deux types de la vie privée (la vie privée de l'emplacement et la vie privée de la requête). Les résultats d'analyse montrent que notre approche peut obtenir un bon équilibre entre QoS et la vie privée.
- ✓ Nous avons utilisé le principe de clique (sous-graphe), parce que les cliques peuvent être rapidement identifiées et utilisées pour générer la région de cloaking lorsqu'une nouvelle requête arrive.
- ✓ Notre approche satisfait la propriété de K-Sharing, pour faire face aux attaques.
- ✓ Dans notre approche, toutes les requêtes seront traitées même si k-1 d'autres utilisateurs ne peuvent pas être trouvés, car nous générons des différents Dummies réels au lieu de rejeter la requête.
- ✓ Pour assurer l'équilibre entre la vie privée de l'utilisateur et la qualité de service, nous adoptons la solution la plus simple et la plus récente qui est le cloaking spatiale.
- ✓ Nous avons évalué les performances et l'efficacité de notre approche proposée par des expériences d'évaluation. Pour générer les utilisateurs mobiles dans notre approche, nous avons utilisé le Thomas Brinkhoff Network-Based Generator Moving Objets [3] sur la carte routière réelle d'Oldenbourg. En plus, les mesures d'évaluation que nous avons utilisées incluent le QoS, la garantie de la vie privée, et la performance. Nous avons ensuite comparé les résultats obtenus avec les autres travaux connexes.

1.5 Organisation de la thèse :

La thèse est organisée en deux parties. La première partie décrite et représente l'état de l'art sur le m-business, la sécurité et la protection de la vie privée, et les travaux connexes (chapitre 2, chapitre 3 et chapitre 4). La deuxième partie est destinée à la représentation et l'évaluation de nos contributions (chapitre 5, et chapitre 6).

Le premier chapitre présente le contexte et la problématique de la recherche. Ce chapitre identifie également les objectifs de la thèse et présente brièvement les principales contributions.

Le chapitre 2 représente l'état de l'art sur le m-business, les déférents types de m-business, et la définition et les caractéristiques de m-busines fournissant de LBS. Le chapitre 3 est un aperçu sur les mécanismes de la sécurité et la protection de la vie privée de l'utilisateur. Dans ce chapitre, nous allons présenter différentes structures du système de protection de la vie privée de l'utilisateur, ensuit, nous présentons les mécanismes de protection de la vie privée de localisation (LPPM). En plus, il présente la classification des attaques sur la vie privée de l'utilisateur dans le m-business.

Le chapitre 4 présente plusieurs travaux existants qui traitent les problèmes de protection de la vie privée de l'utilisateur. Le chapitre 5 présente nos contributions et l'architecture générale de notre approche. Ensuite, nous allons expliquer l'architecture détaillée de chaque composant et son fonctionnement.

Le chapitre 6 montre la mise en œuvre de notre approche, il commence par la présentation des outils et l'environnement de développement. Ce chapitre est consacré à l'exposition de nos expérimentations et résultats des évaluations appliquées sur notre système. Nous terminons la thèse par une conclusion et des perspectives.

Finalement, le chapitre 7 conclus cette thèse. Il synthétise les contributions globales et met en évidence les perspectives de cette recherche.

Chapitre 2

M-business et les services basés sur la localisation

2.1 Introduction

Les techniques mobiles sont aujourd'hui devenues des enjeux majeurs pour l'avenir. Le m-business (business mobile) et son succès et le développement technologique avec l'apparition d'ordinateurs portables, tablettes, téléphones intelligents, connexion 3G, 4G et 5G ... etc., sont autant de facteurs qui changent notre mode de vie. Les technologies mobiles et m-business fournissent une communication supplémentaire et le canal de la transaction, qui peut être appliquée afin d'améliorer les applications existant d'e-business. Dans ce chapitre, nous allons en premier lieu présenter des généralités sur le business mobile ensuite nous allons donner des définitions sur le principe de LBS (location based services) et ses avantages en terme d'optimisation et enfin nous terminerons ce chapitre par une présentation de protection de la vie privée (privacy) et leurs relations avec le business mobile.

2.2 Technologies mobiles

Dans le contexte des technologies mobiles, nous comprenons intuitivement les communications sans fil et les appareils mobiles. Dans la littérature, dans de nombreux cas, sous le terme générique de technologies mobiles, différents types de technologies et d'applications sont discutés, comme par exemple la communication mobile, les services de données mobiles, l'informatique omniprésente, etc. En général, tous ces termes renvoient à une caractéristique commune «communication sans fil» [16].

Les composants de base des technologies mobiles sont les technologies et protocoles de transmission sans fil, tels que Bluetooth, UMTS, WLAN, et différents types d'appareils d'extrémité spécifiquement conçus pour la communication sans fil. Ces terminaux sont par exemple des téléphones portables ou des *assistants numériques personnels*

(PDA) et dans le cas d'une communication machine-machine, cela pourrait être n'importe quel objet équipé de puces spéciales permettant la communication sans fil. Des exemples bien connus de ces puces sont **Remote Frequency Identification RFID**. Les étiquettes *RFID* sont de petites puces capables d'enregistrer et de stocker des données et de communiquer avec d'autres objets en réseau. Les choses sont équipées de RFID appelée choses intelligentes.

2.2.1 Types de la technologie mobile

Les technologies mobiles permettent trois types de communication sans fil :

- ✓ **communication person-to-person :** qui pourrait être une communication vocale ou de données mobile.
- ✓ **communication person-to-machine :** qui fait référence à la communication sans fil de personnes soit avec des serveurs afin de récupérer et de stocker des données, soit avec d'autres choses intelligentes.
- ✓ **communication machine-machine :** c'est-à-dire objet-à-objet, cela est également connu sous le terme d'informatique omniprésente.

2.2.2 Dispositifs mobiles

Dispositif mobile est un appareil informatique portable, qui a souvent un écran et une interface d'entrée-sortie, avec des dispositifs d'interaction nécessaires ou accessoires.

La réalisation de m-business est impossible sans l'utilisation des dispositifs mobiles. Ils varient de manière significative dans leurs capacités, tailles et prix. Les principaux types de dispositifs mobiles utilisés dans le processus de m-business sont les suivants :

- ✓ **Les téléphones mobiles :** ils se caractérisent par la faible capacité de mémoire et le taux de transfert de données. Les téléphones cellulaires de la classe supérieure peuvent être utilisés pour accéder à Internet via les technologies WAP ou GPRS. Ils peuvent également être utilisés pour envoyer et recevoir des messages multimédia (MMS). Leur prix baisse continue.
- ✓ **PDA :** (les assistants numériques personnels) : ils ont de petites tailles et une puissance importante du processeur. Les nouveaux modèles reconnaissent l'écriture manuscrite et peuvent jouer différents types de fichiers multimédia. Les principaux systèmes d'exploitation utilisés sont Palm et Microsoft Pocket PC.
- ✓ **Tablet PC :** Il s'agit de l'un des derniers appareils mobiles. Ils ont la même gamme complète de capacités que les ordinateurs personnels. Certains d'entre eux n'ont pas de clavier mais un logiciel de reconnaissance l'écriture manuscrite. Ils sont relativement coûteux.

- ✓ **Les Smartphones :** ce sont des appareils hybrides qui combinent les capacités des téléphones cellulaires et des PDAs. Ils peuvent reconnaître l'écriture manuscrite. Ils utilisent Symbian, Windows Mobile ou d'autre système d'exploitation. Comme ils ont des navigateurs Internet, ils ont la potentialité d'être utilisés avec succès dans le business mobile. Il est prévu que dans les années suivantes téléphones intelligents seront la meilleure plate-forme mobile pour le m-business.
- ✓ **Les ordinateurs portables :** d'une part, ils ont des capacités identiques à celles de l'ordinateur personnel de bureau ; d'autre côté, ils sont de petites tailles et supportent des communications sans fil. Leurs prix sont encore plus abordables que ceux des ordinateurs fixes.

2.2.3 Inconvénients et les avantages de la technologie mobile

Par rapport à connexion filaire, les technologies mobiles au stade actuel de développement présentent certains inconvénients et certains avantages. Les inconvénients résultent d'une part des petits écrans et claviers des appareils mobiles, d'autre part de leur mémoire limitée et la puissance de calcul. Les caractéristiques spécifiques des dispositifs terminaux mobiles limitent la taille des informations qui peuvent être affichées sur l'écran mobile, rendent la saisie des données difficile et inconfortable, et ne permettent pas un traitement compliqué du côté du client.

Les inconvénients de la technologie mobile décrits ci-dessus sont compensés par les avantages uniques suivants par rapport à connexion filaire :

- ✓ **Ubiquity :** La petite taille des terminaux permet aux utilisateurs de les emporter partout avec eux. Cela vaut également pour les objets avec des étiquettes RFID attachées ou incorporées.
- ✓ **Identification :** Chaque personne ou objet capable de communication sans fil peut être identifiée soit en fonction de l'enregistrement auprès de l'opérateur mobile ou par l'information de l'étiquette RFID ci-jointe.
- ✓ **Localisation :** Chaque appareil mobile ou objet intelligent peut être localisé par les opérateurs mobiles ou en utilisant une autre technologie de positionnement.
- ✓ **Omniprésente** La disponibilité omniprésente de la communication permet une action et une réaction spontanées aux demandes et aux besoins.

2.3 Définitions de Business Mobile

Il existe de nombreuses définitions disponibles pour m-business et m-commerce. Par exemple, [17] définissent une transaction de commerce électronique mobile comme «tout type de transaction d'une valeur économique réalisée par l'intermédiaire d'un terminal mobile utilisant un réseau de télécommunication sans fil pour la communication

avec l'infrastructure de commerce électronique». [18] définissent le commerce mobile comme « ... implique la livraison de produits et de services via de technologies sans fil pour permettre des activités de commerce électronique sans restriction de temps et d'espace ». [19] affirme que « le commerce électronique mobile, communément appelé m-commerce, est la capacité d'acheter des biens n'importe où via un appareil compatible Internet sans fil». [20] a défini le commerce électronique mobile comme «une transaction commerciale d'une valeur économique réalisée à l'aide d'un terminal mobile qui communique via une télécommunication sans fil ou d'un réseau local avec l'infrastructure de commerce électronique». [21] ont fait valoir que les m-business devraient combiner Internet, les technologies sans fil et le business électronique, indiquant que m-business inclut des aspects de l'information, des services et des produits avec des appareils mobiles sur les infrastructures de réseau sans fil.

Les auteurs de [22] définissent m-business comme « la livraison de contenu (notification et reporting) et les transactions (achat et saisie de données) sur les appareils mobiles ».

En outre, les auteurs de [23] ils définissent m-business comme l'utilisation d'appareils mobiles pour communiquer, informer, traiter et divertir à l'aide de texte, de voix et de données par connexion à des réseaux électroniques publics et privés. La mobilité signifie un accès en temps réel et entièrement portable aux mêmes ressources et outils d'information qui, jusqu'à récemment, n'étaient disponibles que depuis le bureau.

Les auteurs de définissent de [24] m-business comme : "Activité Mobile résulte de la capacité de l'individu à avoir un accès permanent à l'information et des services indépendants du lieu et de temps en utilisant un téléphone portable, assistants numériques personnels (PDA) ou PC de poche". Il prend en charge l'échange de biens, services, informations et connaissances. Toutes les transactions sont effectuées via un périphérique mobile.

En plus de la transmission de la voix, l'amélioration des télécommunications mobiles et les technologies sans fil permettent le transfert de données et de contenu à des vitesses raisonnables sur les réseaux radio. Ainsi, il suggère la convergence des technologies Internet à la communication mobile.

La relation spécifique entre la technologie mobile et Internet peut également être observée au niveau de l'application entre e-business et m-business. De nombreuses entreprises ont déjà établi des applications e-business et le canal de communication mobile est considéré comme un canal supplémentaire qui doit être positionné par rapport aux canaux existants [25]. La définition actuelle d'e-business est définie comme suit : "l'intégration de systèmes, de processus, d'organisations, de chaînes de valeur et de marchés entiers utilisant des technologies et des concepts liés à Internet". En conséquence m-business est défini comme un ensemble de technologies et d'applications mobiles utilisées pour soutenir les processus, les chaînes de valeur et des marchés entiers utilisant la technologie sans fil [26].

En résumé, nous pouvons dire que m-business peut être considéré comme un canal supplémentaire pour le business électronique. Toutefois, cela ne signifie pas que les approches de développement d'applications de business électronique peuvent être appliquées au développement d'applications de business mobile sans adaptation [27] et [28].

2.4 Avantages du m-business

La distinction entre m-business et e-business est basée sur les attributs de la proposition de valeur d'ubiquité, de commodité, de localisation et de personnalisation [29]. Bien que les affaires électroniques (e-business) offrent une certaine commodité et personnalisation, le m-business offre des avantages spécifiques en termes de mobilité et de localisation, grâce à la technologie [30].

L'omniprésence des m-business est dérivée des appareils mobiles qui offrent aux utilisateurs la possibilité de recevoir des informations et d'effectuer des transactions à partir de pratiquement n'importe quel endroit en temps réel. Les avantages présentés par l'omniprésence de l'information et l'accès continu aux affaires seront extrêmement importants pour les applications urgentes.

La ***commodité*** est réalisée en termes d'agilité et d'accessibilité fournies par les appareils sans fil. Cela permet également aux m- business de différencier leurs capacités des e-business.

La ***localisation*** de m-business consiste à connaître l'emplacement de l'utilisateur pour créer un avantage significatif, de manière à exploiter les informations spécifiques à l'emplacement en fournissant des informations pertinentes pour la position géographique actuelle de l'utilisateur.

La ***personnalisation*** est réalisée en rendant les appareils mobiles idéaux pour le marketing cible individuel. Lorsque ces quatre éléments sont combinés, le potentiel d'amélioration des activités d'une entreprise devient énorme [30].

2.5 Acteurs de base du business mobile

La capacité à développer une activité de m-business directement dépend de la qualité de l'infrastructure de réseau et du taux d'équipement informatique de la population (par exemple la couverture réseau et les consommateurs doivent disposer d'appareils mobiles). Dans les points suivants, nous allons parcourir les différents acteurs constituant la base du m-business :

- ✓ ***Opérateurs et l'infrastructure réseaux :*** Le client final ne pourrait pas bénéficier des services mobiles sans le transfert de données via les fréquences radio.

Étant donné que l'extension de la couverture réseau permet le développement du m-business, tous les acteurs concernés ont intérêt à favoriser son extension.

✓ ***Systèmes de géolocalisation :*** La possibilité de localiser un utilisateur n'importe où dans le monde provient de deux technologies distinctes. La première méthode est la méthode d'application triangulation en utilisant les données des stations de base pour les opérateurs de téléphones mobiles. Cependant, cette méthode de suivi ne permet pas d'évaluer la position d'un appareil avec la même précision qu'un système GPS (Global Positionning System). Le *système de positionnement global* (GPS) repose sur un réseau de satellites capables de localiser très précisément un appareil à l'aide d'une puce GPS.

✓ ***Terminaux mobiles et les systèmes d'exploitation :*** les terminaux mobiles ne se résument pas aux téléphones portables. Il existe de nombreux supports, avec des utilisations différentes, tels que lecteur de musique numérique, livres numériques ou tablettes numériques. L'utilisation d'un appareil mobile, ils ont toutes les informations disponibles à tout moment et peuvent communiquer avec d'autres appareils via Bluetooth ou WLAN. Le système d'exploitation installé sur le périphérique mobile détermine le canal de distribution des services ; en effet, le système d'exploitation nécessite l'utilisation de son propre applications stores (Google Play, Apple Store etc.). En outre, pour le client final, l'attractivité d'un terminal mobile dépend directement des services et du contenu auxquels il donne accès. En conséquence, les ventes des fabricants de matériel dépendent en partie du système d'exploitation installé sur leurs périphériques.

2.6 Facteurs clés de succès pour le m-business

Le succès du développement du marché de l'm-business dépendra de la capacité des opérateurs à tirer parti des capacités suivantes dans l'environnement mobile :

- ***Propriété du client :***Les données des abonnés, telles que l'adresse de facturation, le numéro de téléphone mobile, l'adresse e-mail, le choix d'un appareil mobile et les habitudes d'appel, sont de plus en plus précieuses à la lumière du business mobile. En plus de la collecte passive des comportements et des données des utilisateurs, les entreprises pourront bénéficier de la participation active des utilisateurs, en précisant leurs propres choix et préférences au fournisseur du portail. Le terminal mobile est le véhicule idéal pour un marketing personnalisé. Les entreprises mobiles peuvent lier des caractéristiques individuelles énoncées à une base de données, qui peut extraire ou déduire des préférences. Par conséquent, les opérateurs de réseaux (surtout lorsqu'ils sont aussi des fournisseurs de services) sont en position de pouvoir exploiter les entrepôts de données qu'ils ont construits au fil des ans.

- ***Personnalisation :***La personnalisation consiste à créer des services qui personnalisent l'expérience de l'utilisateur final pour chaque abonné. Il est basé sur la gestion des relations individuelles et constitue donc l'outil idéal pour le marketing individuel. Une plateforme de personnalisation intelligente doit être en mesure d'apprendre des préférences de l'utilisateur et du comportement passé de l'utilisateur. L'application doit être suffisamment personnalisée pour optimiser le parcours d'interaction, permettant à l'utilisateur d'atteindre les services qu'il souhaite en quelques clics, et la transmission d'informations sous une forme compacte optimisée pour le téléphone intelligent ou le communicateur. Les entreprises doivent également être proactives en ce qui concerne le comportement du service, c'est-à-dire anticiper les besoins futurs de l'utilisateur et suggérer un choix probable.
- ***Localisation :***Il existe plusieurs technologies concurrentes qui permettent des services de localisation ou de positionnement mobiles. Les informations sensibles à la localisation deviennent essentielles dans le business mobile. Connaître l'emplacement de l'utilisateur conduit l'offre de service et d'application à un niveau qui crée une valeur significative pour l'utilisateur. Les utilisateurs ont besoin d'informations locales sur leur environnement local normal. Les informations spécifiques à l'emplacement sont encore plus précieuses dans les nouveaux environnements, lors des déplacements.
- ***Ubiquité :*** La capacité de recevoir des informations et d'effectuer des transactions à partir de pratiquement n'importe quel emplacement est particulièrement importante pour les applications critiques de temps. Il est essentiel de fournir aux utilisateurs mobiles un niveau d'accès et d'information semblable à celui offert dans l'environnement des lignes fixes.
- ***Opportunité :*** Mobile permet la transmission et l'utilisation d'informations sensibles au temps dont la valeur est inhérente à sa livraison immédiate. L'information transmise trop tard peut entraîner des coûts d'opportunité importants.
- ***Commodité :*** Il faut toujours se demander comment une solution pourrait offrir plus de commodité à l'utilisateur. La technologie en elle-même est passionnante, mais seule son utilisation pour améliorer la qualité de vie la rend précieuse.

2.7 Différents types de Business mobiles

Pour cerner les différentes formes de business, il existe une catégorisation fondée sur le type d'acteurs impliqués dans la transaction : le B to B (business to business), le B to C (business to consumer) et le C to C (consumer to consumer).

2.7.1 Business-to-business :

Noté **B2B**, concerne l'utilisation des supports électronique pour tout ou partie des échanges d'information d'une entreprise avec d'autres entreprises : fournisseurs, sous-traitants, clients, partenaires de services, organismes financier. Par opposition à entre une entreprise et un consommateur (voir B2C).

2.7.2 Business-to-Employée :

Noté **B2E**, les entreprises peuvent faire leur intranet accessible à tous leurs agents de terrain, car il (intranet) constitue le support principal des applications B2E. Cela comprend tous les outils d'administration tels que la gestion voyage, carnets d'adresses, ... etc. En outre, toutes les applications d'entreprise sont disponibles sur les appareils mobiles, ce qui nous permet de synchroniser des calendriers, de contrôler les courriels, etc.

2.7.3 Business-to-Consumer :

Noté **B2C**, fait référence à des transactions commerciales dans lesquelles les entreprises vendent des produits ou des services aux consommateurs. Plus récemment, le terme B2C désigne la vente en ligne de produits dans laquelle les fabricants ou les détaillants vendent leurs produits aux consommateurs sur Internet. Le modèle B2C est probablement le modèle que la plupart des gens connaissent. Un aspect révolutionnaire de m-business dans le modèle B2C est la mise en œuvre de services de localisation. Après avoir identifié l'emplacement d'un dispositif mobile, il est possible de fournir à l'utilisateur des informations appropriées selon l'endroit et le temps.

2.7.4 Consumer to Consumer :

Note **C2C**, se réfère à tous les échanges de biens et de services entre plusieurs consommateurs sans passer par un intermédiaire.

2.8 Différences opérationnelles entre M-Business et E-business

La différence opérationnelle fondamentale entre l'e-business et m-business réside dans l'interaction des utilisateurs. Dans le business électronique, les utilisateurs interagissent avec des ordinateurs de bureau. Dans M-business, les employés peuvent interagir de n'importe où, même lorsqu'ils sont en déplacement. E-business est un système basé sur le Web sur les ordinateurs personnels et les serveurs, tandis que m-business est un système basé sur les appareils mobiles. Dans m-business, les employés accèdent à la

productivité et à d'autres solutions à partir de téléphones mobiles et d'autres appareils portables [31].

- ***Flexibilité :*** le m-business offre plus de souplesse que l'e-business. Les employés peuvent faire leur travail pendant leurs déplacements ou leurs voyages d'affaires. Les gestionnaires peuvent tenir des réunions virtuelles avec leurs employés à temps plein et leurs consultants indépendants, dont certains travaillent peut-être à domicile. Les profils d'utilisateur peuvent être transférés de manière transparente du bureau à l'appareil mobile, et le transfert rapide des données peut avoir lieu entre les deux. Cependant, cette flexibilité dépend d'une connexion réseau rapide et fiable, car m-business s'arrête en cas de panne du réseau mobile.
- ***Prestation de service :*** La prestation des services d'e-business se fait habituellement par Internet ou par réseaux d'entreprises privées sécurisés. M-business permet aux entreprises de déplacer une partie de ses capacités dans ses emplacements de terrain

2.9 Principaux problèmes et défis du m-business

L'environnement de m-business présente un nouvel ensemble de problèmes ou de défis auxquels l'industrie est confrontée. Bien que le m-business soit intrinsèquement un domaine technologique, elle devrait avoir de profondes répercussions sur la vie quotidienne des gens, les entreprises et la société dans son ensemble.

Dans cette section, nous présentons les principaux défis de m-business.

✓ **Smartphones (PDA) : un canal de communication :** Un smartphone, un objet situé entre un téléphone et un ordinateur, n'est pas simplement un navigateur d'Internet ou un outil permettant d'acheter en ligne. Mais c'est aussi un moyen de communication, qui est essentiellement sa fonction principale. Cette détermination est un facteur important et doit être prise en compte pour une entreprise. En fait, cela nous permet de contacter des clients. Nous pouvons déjà envoyer des MMS et des SMS pour promouvoir des produits ou des marques spécifiques ou visiter le magasin. Une étude [32] indique que 68% des Américains aux États-Unis communiquent quotidiennement par SMS et que ce sont parfois les entreprises ou les marques qui qui utilisent ce mode de communication pour des communications privilégiées avec leur cible. Même si le smartphone devient un assistant personnel du grand public, il permet de faire des shoppings, de bénéficier de réductions et d'avoir un GPS pour trouver l'itinéraire à suivre ou encore obtenir les coordonnées d'un professionnel, etc. De la même manière, il est important de mettre le code QR dans différentes méthodes de communication : SMS, email, etc. Le code QR est un code-barres de forme carrée en 2D qui peut être scanné et déchiffré rapidement, contrairement aux codes à barres traditionnelles ;

il contient plus d'informations, ce qui l'amène à des informations ciblées que vous n'auriez pas trouvées ailleurs, mais qui nécessiteraient un téléphone portable avec un lecteur de code QR. Le smartphone dispose de nombreuses fonctionnalités permettant aux entreprises d'atteindre leurs objectifs, telles que la messagerie électronique. En fait, selon une étude [33], 49% des utilisateurs de smartphones consultent leurs emails via leur téléphone portable au moins une fois par jour. Il est donc important de garder à l'esprit que les courriels peuvent être lus sur un téléphone portable tout en soulignant les informations pertinentes.

✓ **Protection de la vie privée :** Les utilisateurs ne veulent une transmission et une utilisation sans protection de leurs données personnelles qui sont souvent utilisé pour établir le profil d'un utilisateur. Une enquête a montré que les utilisateurs n'étaient pas très rassurés mais ils étaient aussi peu conscients de l'ampleur des collectes et transmissions de données personnelles, mais de nombreux utilisateurs ont estimé que les données personnelles ne sont ni transférées ni collectées à leur insu. Selon une étude [33], «le smartphone exporte en moyenne 144 000 requêtes par jour vers plus de 300 serveurs répartis dans le monde !» et lorsqu'il est en veille, il envoie en moyenne 30 000 à environ 80 serveurs, sachant qu'ils sont essentiellement des serveurs étrangers. Ce qu'il faut savoir aussi c'est qu'environ 30% des applications accèdent à la localisation mais les utilisateurs ne savent pas forcément la raison pour laquelle la localisation doit être activée telles que Apps Jeux, réseaux sociaux etc. On peut supposer que de nombreux fournisseurs souhaitent connaître la position de leur cible pour mieux répondre aux besoins et aux attentes de celui-ci afin d'adapter son offre par exemple. La géolocalisation permet d'améliorer la gestion de l'entreprise et de réaliser des économies. Mais la géolocalisation ne doit pas être utilisée à des fins malhonnêtes par ses employés ou ses clients.

✓ **Importance de la géolocalisation :** La géolocalisation est utilisée pour positionner une personne sur une carte à l'aide de coordonnées géographiques. Dans la géolocalisation mobile, la localisation se fait à l'aide des opérateurs mobiles qui utilisent ces deux technologies qui sont : le GPS et le GSM qui signifie l'utilisation des ondes radio. Aujourd'hui, tous les opérateurs de téléphonie mobile offrent l'accès à cette option. La géolocalisation est un service très agréable, efficace et pratique qui a attiré de nombreux utilisateurs. Ainsi, la géolocalisation sur mobile situé géographiquement les utilisateurs et leur téléphone portable. En plus, la géolocalisation est aussi très utilisée dans les applications qui sont utilisées quotidiennement telles que les réseaux sociaux et les jeux. La géolocalisation gratuite est incluse dans tous les forfaits mobiles offrant un accès à Internet. Ainsi, les services offerts sont variés mais peuvent avoir des options géolocalisées qui sont payants, mais les plus célèbres sont la navigation routière, le guide de la ville, les

prévisions météorologiques et les plans de quartier. Cependant, la géolocalisation permet également de localiser des points de vente, des restaurants, des librairies, ainsi que des personnes telles que vos parents, vos amis, etc. Cette option permet donc d'orienter les utilisateurs vers les magasins. Mais cela peut aussi être un canal de communication pour distribuer d'offres promotionnelles ou même être un moyen publicitaire. La géolocalisation peut recueillir des informations, des opinions ou des suggestions des utilisateurs. Ces démonstrations montrent que les applications mobiles utilisant la géolocalisation est l'intermédiaire entre les magasins et les clients [34].

2.10 L'importance de la localisation dans le m-business :

Le m-business a un impact considérable sur notre vie et nos affaires. Connaître la position physique d'un utilisateur à un moment donné peut représenter un énorme potentiel pour les fournisseurs de services. Ce service permet aux utilisateurs mobiles d'utiliser des services en fonction de leur emplacement géographique [35].

En plus, avec les progrès des technologies de communication sans fil et de positionnement mobile, les services basés sur la localisation (LBS) ont été largement adoptés, tels que la santé, indoor object search, le divertissement, la vie personnelle, etc. Ces applications offrent aux utilisateurs une grande commodité, et améliorent considérablement la qualité de travail et la vie personnelle [36]. Pour cette raison, le m-business présente de nouvelles fonctionnalités par rapport au business électronique classique, notamment la mobilité, l'instantanéité, la personnalisation et la commodité [37].

En outre, les services basés sur la localisation reposent sur le partage des informations de localisation d'un utilisateur avec un ensemble d'individus spécifiés appartenant à leur famille, leurs amis ou leurs associés. Ainsi, il existe des services permettent ce type de partage tels que Google Latitude, Glympse, Foursquare ou Gowalla [38]. Les services basés sur la localisation ont dominé les marchés du business mobile. Voici quelques exemples des applications de m-business : Route Guide, Push/Pull Advertising, Friend Finders et Location Sensitive Billing [35].

Par conséquent, l'emplacement est très important pour la vie humaine qu'il est essentiel pour la façon dont les gens organisent leur environnement. C'est une valeur essentielle que nous pouvons facilement exploiter pour modéliser la réalité [35]. De ce fait, par rapport à l'e-business, le m-business est une activité de plus en plus axée sur la localisation dans laquelle les informations de localisation sont utilisées [38]. Il y a aussi un groupe de services en constante évolution qui peuvent être fournis aux personnes en fonction de leur localisation. Par exemple, il peut être demandé aux utilisateurs recherchant un service particulier de fournir leurs informations de l'emplacement afin de fournir des informations plus spécifiques sur les services les plus proches. À l'aide de services de localisation, les utilisateurs peuvent demander des informations sur les sites

touristiques à proximité ou sur l'emplacement d'autres services. Ils peuvent également recevoir une aide d'urgence et autres, en fonction de leur emplacement [38].

2.11 Les services basés sur la localisation (LBS)

2.11.1 Définition de LBS

Les services basés sur la localisation (LBS), également appelés services de localisation, service mobile basé sur la localisation, services de localisation sans fil, constituent une technologie innovante qui fournit des informations ou les rend disponibles en fonction de la localisation géographique de l'utilisateur [35].

En plus, le LBS est une classe générale de services d'information accessibles aux clients mobiles, utilisent des informations sur les emplacements géographiques d'appareils mobiles basées sur des technologies de communication mobile telles que GPS [37].

2.11.2 Détermination de l'emplacement d'un utilisateur

Les services basés sur la localisation reposent sur des informations relatives à la localisation d'un utilisateur. Ces informations sont généralement collectées et communiquées par des appareils mobiles que les utilisateurs emportent avec eux ou qui sont situés dans un véhicule conduit par l'utilisateur. En plus, la capacité de communiquer des informations sur leur emplacement est généralement essentielle au bon fonctionnement d'un appareil. Par exemple, un téléphone mobile ne peut ni envoyer ni recevoir d'appels sans communiquer continuellement des informations sur son emplacement [38].

Selon la technologie utilisée, il y a différentes façons de déterminer l'emplacement d'un appareil. Un moyen de déterminer l'emplacement d'un appareil repose sur l'infrastructure réseau et différentes technologies de positionnement (telles que Wimax, Wi-Fi, UWB et RFID). Cette méthode est utilisée avec des appareils mobiles sans GPS intégré, où la position de l'appareil est estimée par rapport à la base, ou nœuds de balise. Le processus commence par l'estimation de la distance et l'angle entre l'appareil et plusieurs nœuds de balise dans son voisinage, soit par le dispositif lui-même, ou par le service de réseau. Ensuite, la position de l'appareil est ensuite calculée en appliquant un ou plusieurs des principes géométriques fondamentaux de la trilatération, de la multilatération et de la triangulation [38].

En outre, la distance peut être calculée en étudiant les signaux reçus. Lorsque l'utilisateur de l'appareil est en mouvement, la direction du mouvement peut être déterminée par l'angle du signal reçu, ou en utilisant des capteurs de mouvement tels que des accéléromètres.

La trilatération est une technique utilisée pour déterminer la position relative d'un point, ou d'un appareil mobile en utilisant la géométrie des triangles tout comme la

triangulation. Cette méthode peut être comparée à la triangulation, qui consiste à mesurer les angles entre l'emplacement de l'appareil et trois balises ou plus, avec des emplacements connus ou fixes. Cependant, la localisation d'un objet par multilatération implique le calcul de la différence de temps d'arrivée d'un signal émis par cet objet à trois récepteurs ou plus. Par conséquent, une ou plusieurs de ces méthodes peuvent être utilisées pour identifier l'emplacement du périphérique [38].

Une autre méthode pour déterminer l'emplacement d'un appareil mobile est l'utilisation du GPS et de l'A-GPS (Assisted GPS) une technologie utilisée pour augmenter les signaux GPS. Ceci est utile dans les zones urbaines ou les lieux intérieurs où les signaux peuvent être faibles. Par conséquent, un appareil est compatible avec le GPS peut transmettre les informations capturées par les satellites via le réseau cellulaire au serveur de localisation, qui les retransmettra ensuite à l'appareil mobile. En outre, la technologie GPS peut être combinée avec d'autres technologies de localisation pour produire des informations de localisation plus précises [38].

Les téléphones intelligents (Smart phones) et autres appareils mobiles de ce type émettent des informations de localisation toutes les quelques secondes. Ce processus se produit de façon répétée afin que l'appareil soit toujours au courant de son emplacement par rapport aux tours de communication et l'utilisateur ne subisse aucun retard dans la réception ou la transmission des appels. En outre, les utilisateurs peuvent ne pas être conscients que ce processus de communication des informations de localisation est rapide, régulier et continu.

Plus récemment, les points d'accès Wi-Fi ont été utilisés pour déterminer l'emplacement d'un périphérique. Les points d'accès Wi-Fi émettent continuellement leurs informations de localisation sous la forme d'une adresse MAC (Media Access Control). Les systèmes de positionnement Wi-Fi (WPS) collectent et cartographient l'emplacement des points d'accès Wi-Fi. Lorsqu'un utilisateur utilise un appareil mobile, l'appareil cherche des points d'accès Wi-Fi à proximité. L'emplacement de l'appareil peut être calculé en fonction des points d'accès visibles par l'appareil. Au cours de ce processus, des périphériques individuels peuvent également être identifiés par leurs propres adresses MAC [38].

2.11.3 Avantages des services basés sur la localisation

Un avantage principal d'utilisation les services de localisation est la possibilité de filtrer de grandes quantités de contenu disponibles sur Internet et de ne fournir que les informations intéressantes à l'utilisateur. Par exemple, une simple demande de service ne fournit pas tous les services enregistrés à l'utilisateur. Donc, il ne fournit que les services les plus proches, afin d'éviter le filtrage. Ainsi, les fournisseurs retournent des informations concernant uniquement les services situés dans le voisinage immédiat de l'utilisateur.

Par conséquent, la connaissance de l'emplacement peut également permettre une variété d'avantages en matière de santé et de gestion des urgences. Le potentiel de développement de services de localisation est pratiquement illimité et peut s'étendre à tous les domaines de l'activité humaine.

Cependant, le partage des informations de la localisation peut également avoir une dimension non consensuelle. Dans les sections ci-dessous, nous allons présenter les problèmes de la vie privée de l'utilisateur.

2.11.4 Principaux problèmes de sécurité dans le m-business :

La sécurité peut être divisée en un certain nombre de problèmes clés, comme suit [39] :

confidentialité

- ✓ **Confidentialité :** La confidentialité des informations sensibles telles que les détails de carte de crédit doit être protégée. Les personnes non autorisées ne devraient pas pouvoir accéder à des documents confidentiels.
- ✓ **Intégrité :** Les entreprises doivent protéger l'intégrité des données transmises sur les réseaux sans fil, du point de transmission au point de livraison. Ceci est particulièrement essentiel pour les transactions financières. Ainsi, par exemple, si un utilisateur entre un paiement de 10 $, ce montant ne doit pas acquérir un zéro supplémentaire en transit. Pour faire face à ce risque, il doit être possible de vérifier que les données sont les mêmes aux points d'origine et de destination.
- ✓ **Disponibilité :** Il s'agit de s'assurer que les données et les services sont disponibles sur demande, ce qui signifie souvent 24 heures par jour, sept jours par semaine. Cela est étroitement lié à la sécurité, car une faille de sécurité peut entraîner des interruptions, comme dans le cas d'attaques par déni de service et de virus. Si les systèmes ne sont pas sécurisés contre les interventions non autorisées (malveillantes ou non), il y a un risque que leurs services ne soient pas fiables et que la productivité des employés ou la satisfaction des clients en souffrent.
- ✓ **Vie privée :** En plus de ces problèmes de sécurité bien établis, la vie privée est un problème majeur dans le business mobile, en particulier avec le développement de services basés sur la localisation (LBS). En plus, le m-business fournit des services basés sur la localisation, ce qui permettra aux utilisateurs d'être suivis. Cela introduit de nouvelles préoccupations concernant la vie privée pour les consommateurs.

La capacité de surveiller en permanence la position d'un individu en temps réel est une préoccupation critique de la vie privée. On peut révéler beaucoup d'informations sur sa vie privée. Les utilisateurs mobiles peuvent être suivis sans le savoir, ce qui peut

avoir des conséquences dangereuses. Certaines lois sur la confidentialité de l'emplacement sont mises en place pour limiter l'utilisation des informations de localisation. Les détails incluent que les entreprises ne peuvent utiliser les informations de localisation que selon les souhaits de l'utilisateur ; les entreprises devraient demander aux utilisateurs la permission d'exposer leurs informations à des tiers ; les utilisateurs devraient être informés de la collecte de leurs informations. Toutefois, il doit redoubler d'efforts pour empêcher le vol et l'utilisation illégale d'informations de localisation [35].

2.12 Protection la vie privée et m-business

2.12.1 Définition de la vie privée :

Le concept de vie privée fait toujours référence au terme anglais "Privacy", qui fait référence à la définition de *Westin* « Le droit à un individu de déterminer lui-même quand, comment et dans quelle mesure ses informations seront divulguées aux autres» [40]. Par conséquent, le droit à la vie privée assure à un individu la capacité de se cacher et se protéger, ou protéger ses informations personnelles. Cependant, ce qui est privé dépend d'un individu à l'autre, bien qu'il existe quelques exigences communes.

En d'autres termes, la vie privée est la capacité d'un individu à contrôler l'accès à ses informations et à conserver son anonymat. C'est parce que, la personne est l'unique propriétaire de ses informations et renseignements, et seule la personne à avoir le droit de décider de les divulguer ou non. La plupart des personnes pensent que la vie privée est précieuse et difficile à récupérer en cas de perte causée par des manœuvres inadvertance ou par intentionnelles.

En conséquence, les procédures de la vie privée sont toutes les actions qui interfèrent dans l'intimité de la personne, y compris la surveillance de ses activités et l'enregistrement ou le traitement de ses informations personnelles.

2.12.2 principes fondamentaux de la vie privée

Nous discutons dans cette partie les critères les plus utilisés. Selon CCITSE "Common Criteria for Information Technology Security Evaluation" [41], il existe quatre critères suivants :

- **Pseudonymie :** Les autres utilisateurs ne peuvent pas associer l'identité de l'utilisateur à une action particulière, dans ce cas l'utilisateur est responsable de ses actions.
- **Anonymat :** Un utilisateur peut utiliser une ressource ou un service sans révéler son identité.
- **Non-associabilité :** L'utilisateur peut effectuer de nombreuses actions sans que les autres soient en mesure de les relier ensemble.

- **Non-observabilité :** L'utilisateur peut utiliser une ressource ou un service sans que les autres soient en état de constater que la ressource ou le service est utilisé.

les auteurs [42] essayent de mettre une terminologie intégrale en ce qui concerne la vie privée. En plus, dans [42] les auteurs rajoutent les critères suivants à ce qui a déjà été défini par CCITSE :

- **Gestion des identités :** Un attaquant ne peut en aucun cas associer le pseudonyme de l'utilisateur à son identité réelle.
- **Indétectable :** Le caractère indétectable d'un objet d'intérêt (IOI) du point de vue d'un attaquant signifie que celui-ci ne peut pas distinguer suffisamment s'il existe ou non. Autrement dit, un attaquant ne peut détecter si un point d'intérêt commun à plusieurs utilisateurs existe.

2.12.3 Menaces à la vie privée

Les données doivent d'abord être collectées, puis supprimées avant qu'elles ne soient présentes et utilisées dans un système.

2.12.3.1 Collecte des données

Lors de la collecte des données, le service doit s'assurer que l'utilisateur comprend que ses informations seront collectées, tout en lui expliquant les raisons de son utilisation. Par conséquent, les données ne doivent pas être collectées sans son accord et il doit être complètement conscient des données fournies [43]. En outre, les données collectées doivent être réduites au minimum et le fournisseur de services doit collecter les données nécessaires à l'utilisation [44].

Un autre point est les risques d'inférence des données et les techniques désanonymisation. Il existe des études ont montré que les données anonymes peuvent être regroupées et analysées avec d'autres données pour d'identifier les personnes concernées ce qui contredit le critère de la nonassociabilité [45].

2.12.3.2 Utilisation des données

Après la collecte et le stockage des données d'utilisateur, les données ne doivent pas être utilisées à des fins autres que celles présentées à l'utilisateur, par conséquent, le système doit assurer le respect du contrat d'utilisation. Le système doit également assurer la protection l'identité et les données de l'utilisateur, tout en lui permettant un contrôle total sur comment ses données sont révélées.

Parfois, les mesures minimales de sécurité ne sont pas appliquées ou insuffisantes pour protéger les données stockées.

2.12.3.3 Effacement des données

Les données d'utilisateur doivent être supprimées après la suppression de l'utilisateur du système, et ce n'est pas une tâche facile, en raison de la quantité souvent énorme de données stockées. Par conséquent, le système doit garantir que les données sont supprimées dans un délai limité et doit assurer le droit à l'oubli à ses utilisateurs.

Certains fournisseurs de services conservent les données et l'historique de recherche de leurs clients le plus longtemps possible afin de récolter les habitudes d'achats et de les exploiter grâce au forage des données [46]. Notons que le fait de garder les données augmente les risques de mauvaise utilisation.

2.12.4 vie privée et implications des services de localisation

Les applications m-business fournissant les services de localisation représentent une large catégorie des services en ligne ; et leur développement rapide au cours des dernières années est l'une des principales raisons de leur participation à la vie des individus. En plus, les implications des services de m-business touchent directement à la vie privée des clients. Nous détaillons dans la suite les implications sur la vie privée.

Le développement de services basés sur la localisation a des implications de grande portée en ce qui concerne le droit à la vie privée des individus. Dans le m-business, les nouvelles informations concernant des personnes (à savoir les informations de localisation) seront traitées par des fournisseurs de services qui sont susceptibles d'être pas fiables (indigne de confiance). De plus, ces informations seront combinées avec des renseignements sur les clients, ce qui augmente le risque que des personnes perdent le contrôle de leurs informations personnelles et sensibles [39].

Pour aller plus loin, un appareil mobile pourrait être utilisé sur une période donnée pour suivre la position d'un individu et pour développer un profil de ses mouvements (par association, ses habitudes). Aujourd'hui, les informations de localisation sont devenues plus précises, tandis que la connectivité permettra potentiellement une traçabilité 24 heures sur 24 [39].

Par conséquent, ce type d'information est très utile, mais s'il est utilisé de façon abusive, cela peut être très dangereux pour la relation client. Étant donné de la sensibilité de ce type d'information, les utilisateurs voudront savoir que leurs informations sont entre de bonnes mains avant d'envisager l'adoption des services de m-business [39].

Cependant, on ne peut pas ignorer les avantages des services de m-business, ce n'est pas à cause des risques qu'ils peuvent porter à notre vie privée, que nous devons les éliminer tous de nos appareils mobiles.

2.13 Problématiques de la vie privée

« Les données de localisation racontent une histoire détaillée». Il ne fait aucun doute que le développement explosif des applications m-business basées sur la localisation présente une nouvelle série de problèmes relatifs à la vie privée des utilisateurs. L'utilisation d'appareil mobile équipé d'un système GPS comme les téléphones intelligents et les tablettes est devenue omniprésente. En outre, l'utilisation des informations de localisation ou une combinaison ces informations avec d'autres informations peuvent révéler une quantité excessive de renseignements personnels sur les utilisateurs [38].

En général, toutes sortes d'informations peuvent être reliées à un emplacement géographique, comme les données financières, les données sur la santé et d'autres données sur le comportement des utilisateurs. Par conséquent, cette information peut comprendre des détails que la personne n'avait pas l'intention de partager.

Dans cette section, nous examinons d'abord les attitudes des utilisateurs envers la vie privée de la géolocalisation avant de donner un aperçu de certains des problèmes de la vie privée soulevés par l'utilisation de ces technologies.

2.13.1 Préoccupations et les attitudes des consommateurs

Le rapport de FTC des États-Unis (The U.S. Federal Trade Commission) a observé que «malgré le manque de compréhension des consommateurs sur la manière dont les entreprises collectent et utilisent leurs données, les consommateurs se soucient de leur vie privée». En plus, ce rapport identifie la sensibilisation des consommateurs comme un facteur clé dans le traitement des problèmes de la vie privée (privacy issues). Par conséquent, lorsque les consommateurs sont conscients des risques d'atteinte à la vie privée et des moyens efficaces pour les résoudre, ils prennent de telles mesures. Cependant, l'investissement de temps et d'efforts requis par les consommateurs pour protéger leur vie privée peut décourager leur volonté de prendre ces mesures [38].

Les utilisateurs sont moins à l'aise de partager leurs informations de localisation lorsque leur position est révélée en temps réel et lorsqu'ils n'ont aucun contrôle sur les personnes qui ont accès à ces informations. Cela indique que les informations claires et accessibles, ainsi que les outils de protection de la vie privée efficaces, sont des éléments importants d'une protection appropriée de la vie privée.

Il y a plusieurs risques de la vie privée associés aux applications de m-business fournissant des services basés sur la localisation. Dans les sous-sections ci-dessous, nous discutons et mettons en évidence certaine de ces risques.

2.13.1.1 Partage d'informations par les utilisateurs

Il existe de nombreuses applications permettant aux utilisateurs de partager leur emplacement avec d'autres personnes. Généralement, ses «autres» sont sélectionnés par

la personne qui choisit de divulguer ses informations. Par exemple, un utilisateur peut identifier certains amis ou membres de la famille qui peuvent accéder à ses informations de localisation.

Cependant, dans certains cas, cette capacité de choisir peut être annulée par des paramètres par défaut. Par exemple, l'application «Places» de Facebook partagera automatiquement les informations de lieu avec tous les amis de l'utilisateur après l'enregistrement dans un lieu, à moins que cette fonction ne soit désactivée par l'utilisateur. Étant donné que beaucoup de gens ont un grand nombre d'amis, un défaut général de cette nature augmente le risque que des informations de localisation soient divulguées par inadvertance à des personnes avec lesquelles on préférerait ne pas partager.

Par conséquent, la divulgation des informations de localisation sans la connaissance de la personne concernée crée un ensemble de différents risques pour la vie privée. Non seulement les individus deviennent vulnérables au harcèlement criminel ou à tout autre contact non désiré, mais les informations de localisation peuvent permettre de partager par inadvertance des informations sur des activités sensibles (visites de cliniques médicales ou réunions politiques, par exemple).

La fonction de protection de la vie privée est souvent présentée comme la capacité de contrôler qui peut accéder à l'information de localisation. Cependant, même si un utilisateur est au courant et exerce ces contrôles, il peut toujours y avoir des risques. Les informations peuvent également tomber entre les mains des autres lorsqu'un appareil est perdu, prêtées ou volées.

Des rapports récents indiquent que l'iPhone 4 a sauvegardé et stocké des renseignements détaillés sur l'emplacement sur les disques durs des utilisateurs sans préavis ni consentement. Ces données seraient accessibles à toute personne ayant accès à l'ordinateur [47].

L'utilisation des appareils prenant en charge de nombreux systèmes de positionnement, tels que GPS et GLONASS, peut également entraîner la collecte, l'utilisation et la divulgation d'informations de localisation à des fins qui ne sont pas directement liées à la fourniture d'un service de localisation particulière. Bien que les informations de localisation peuvent être nécessaires pour fournir des services de communication mobile, leur stockage à long terme n'était pas nécessaire pour la fourniture du service.

2.13.1.2 Profilage des données (profiling)

Le profilage de données est le processus consistant à récolter les données disponibles d'une source d'information existante (par exemple, une base de données ou un fichier) et à collecter des statistiques ou informations sur ces données. C'est ainsi très proche de l'analyse des données [48].

Par conséquent, les informations de localisation collectées (ou partagées) via les appareils mobiles peuvent être très révélatrices les mouvements et les activités des

individus. Parce que, les appareils mobiles ont tendance à être très étroitement associés à des individus spécifiques. En plus, les informations révèlent également des modèles d'activité et d'inactivité, permettant de tirer d'autres conclusions. Par exemple, les informations peuvent révéler qu'ils ont fait des visites fréquentes dans une clinique ou un hôpital. Cela permet au fournisseur de services basés sur la localisation d'avoir un aperçu intime des habitudes du propriétaire d'un tel appareil et de créer des profils étendus.

En outre, les fournisseurs de services basés sur la localisation ou de services connexes sont souvent en mesure de suivre ou d'enregistrer les mouvements de leurs utilisateurs avec une grande précision spatiale et temporelle [47]. En conséquence, ils peuvent générer un historique complet des mouvements de chaque utilisateur, y compris le type de services auxquels ils ont accédé et le moment de l'accès [49].

Cependant, il est clair que les informations personnelles de ce type ont une valeur commerciale. Il existe également des entreprises qui conservent les informations aussi longtemps que possible pour une exploitation commerciale future de ces informations [47].

L'un des moyens d'exploiter de telles informations est le profilage des données. Le profilage des données des consommateurs est déjà une industrie majeure et il ne fait aucun doute que plus les données sont détaillées, plus leur utilité commerciale est grande [50].

En conséquence, les informations sur l'emplacement, les mouvements et les habitudes d'activité peuvent constituer des éléments précieux de tout profil de données. De plus, les informations sur une personne peuvent être inférées en fonction de leurs habitudes de mouvement, même quand ils agissent de façon anonyme [38].

Les services de localisation fournis par le m-business peuvent créer un enregistrement chronologique dans le temps en fonction des données transmises, permettant ainsi un lien entre les enregistrements et l'utilisateur réel. Par conséquent, l'emplacement ou le lieu géographique peut constituer un identifiant puissant.

2.13.1.3 Sensibilité des données de localisation (géolocalisation)

Les informations de localisation (géolocalisation) ont toujours été identifiées comme une information personnelle, ou du moins connue uniquement par des proches. En plus, ne peut pas ignorer les conséquences négatives de sa divulgation. Par conséquent, la combinaison des informations de localisation et d'autres informations personnelles peuvent être moyen précis pour identifier des individus par des individus potentiellement malveillants. De même, la position d'un utilisateur peut révéler ses intérêts et faciliter son identification [51], [52]. En outre, la perception des risques par les utilisateurs est considérée comme l'un des problèmes majeurs [53].

2.13.1.4 Perte de contrôle sur les données personnelles

L'utilisation des nouvelles technologies est une partie essentielle de notre vie quotidienne et par conséquent de nouveaux produits et services sont proposés tous les jours. Dans la littérature, des chercheurs de nombreux domaines ont tenté d'étudier l'impact de LBS sur la vie privée des utilisateurs. Les utilisateurs ne sont pas conscients des risques associés au partage de leurs informations en ligne. De même, les utilisateurs sont plus disposés à divulguer des informations personnelles sur les réseaux sociaux que d'autres sites, c'est pour cela le comportement des individus vis-à-vis de la vie privée est malléable selon le contexte de l'interaction. En plus les utilisateurs divulguent leurs informations quand ils voient les autres le faire [54].

D'autre part, les utilisateurs ne sont pas vraiment conscients de la valeur de leurs données et les divers risques associés à la divulgation en ligne [55]. En fait, la plupart des utilisateurs croient à tort que si un site a une politique de confidentialité, ils ne pourront pas partager leurs informations personnelles avec les autres. De même, il y a d'autres qui croient que les entreprises ne sont pas intéressées par ce qu'ils font en ligne. Des études ont montré que certains utilisateurs ont désinstallé des applications mobiles après ils ont appris que ces applications bénéficiaient de leur géolocalisation. La plupart préfèrent désactiver l'accès à l'emplacement au lieu de désinstaller complètement l'application [56].

Cependant, il existe d'autres études ont aussi montré que les utilisateurs accordent l'accès aux applications pour lesquelles les informations de localisation sont nécessaires pour leur fonctionnement et empêchent l'accès lorsque les objectifs d'utilisation sont moins clairs. D'autres facteurs affectent également l'intention de partager l'emplacement comme par exemple l'endroit où l'utilisateur se trouve, l'activité ou la relation avec le demandeur (famille et amis) [57].

Malgré le fait qu'il est difficile d'identifier tous les problèmes de vie privée dans le m-business fournissant les services de localisation, nous avons essayé de surligner les problèmes relatifs à la divulgation des informations de la localisation. En outre, de nombreuses recherches et travaux ont été réalisés pour aborder certains des problèmes de vie privée.

2.14 Intégration avec système d'information géographique

2.14.1 Système d'information géographique SIG

Le système d'information géographique (SIG) est un système informatique conçu pour saisir, stocker, manipuler, analyser, gérer et afficher les différents types de données spatiales ou géographiques [58].

La partie «géographique» du SIG fait référence à des informations sur les positions à la surface de la Terre, également appelées données spatiales, car elles peuvent être localisées dans l'espace et avoir une référence géographique. Un exemple de données spatiales est l'adresse de domicile. En général, les systèmes d'informations sont utilisés pour manipuler, résumer, interroger, modifier et visualiser les données, SIG fait toutes ces choses avec des informations spatiales [58].

2.14.2 M-business et SIG

Dans le m-business, les services basés sur la localisation sont largement adaptés, de même que les systèmes de positionnement global (GPS) et les systèmes d'information géographique (SIG). Les entreprises de m-business peuvent identifier l'emplacement physique de leurs clients lorsqu'ils utilisent leurs appareils mobiles [59]. La position peut être combinée avec des informations spatiales afin d'intégrer le système m-business avec des systèmes d'informations géographiques (SIG) ou d'autres informations dépendant de la localisation [60].

Dans le m-business, le fournisseur de services traite des données géographiques. La présentation de cartes sous diverses formes est basée sur le développement de connaissances cartographiques sur la conception de cartes. Plusieurs aspects importants d'un SIG doivent être analysés lorsqu'on essaie d'améliorer un système m-business avancé avec des fonctionnalités SIG, telles que la collecte, la conversion, la gestion, l'analyse et la présentation de données géographiques [60].

La puissance des systèmes m-business fournissant LBS réside dans la fourniture de fonctionnalités SIG et d'informations géo-localisées sur des réseaux fixes et mobiles tels que la collecte, la conversion, la gestion, l'analyse et la présentation de données géographiques, pour être utilisé par n'importent qui, n'importe où, à tout moment et sur n'importe quel appareil.

Le SIG mobile et le m-business ont des exigences particulières sur la présentation des cartes et sur l'interaction avec les objets spatiaux, qui résultent de la position et de l'orientation variables de l'utilisateur et des applications typiques réalisées sur les appareils mobiles [3]. Les caractéristiques d'un SIG mobile sont la mobilité et l'interconnectivité via des réseaux sans fil, tout en utilisant certains serveurs d'informations géographiques (SIS). Les technologies analytiques, de stockage et d'extraction et de collecte de données ne sont que des technologies au service de base.

2.15 Conclusion

Comme toute innovation, l'apparition des services de m-business a donné lieu à un ensemble d'opportunités et d'applications nouvelles. Aujourd'hui, les m-business sont partout présents en nombre. Dans ce chapitre, nous avons présenté la définition de m-

business, les services dans le m-business et les avantages et améliorations de m-business par rapport à e-business. Puis nous avons présenté les technologies de communication et les dispositifs mobiles, les obstacles et les défis de m-business. En plus, nous avons présenté les services LBS et la protection de la vie privée dans le m-business.

Dans le prochain chapitre, nous allons donner un aperçu sur la protection de la vie privée dans le m-business qui fournit les services LBS. Ensuite, nous allons présenter quelques comparaisons entre les différentes structures du système de protection de la vie privée de client dans le m-business.

Chapitre 3

Protection de la vie privée

3.1 Introduction

La prolifération des appareils mobiles compatibles avec la localisation entre les mains des consommateurs a entraîné un développement rapide des services basés sur la localisation. Les emplacements de client représentent des données personnelles. En outre, les fournisseurs de services non digne de confiance peuvent recueillir ces données et l'utilisation abusive. La collecte et l'utilisation de telles données sont donc soumises aux règles de vie privée.

Le problème de la protection de la vie privée (Privacy) se pose parce que les emplacements sont collectés par les fournisseurs de services LBS. Malheureusement, l'utilisation de l'approche traditionnelle du pseudonymat (fausse identité) ne permet pas de surmonter une telle menace pour la vie privée dans le m-business, où les emplacements personnels peuvent être utilisés comme identités. Par exemple, le fait de poser des requêtes sur le service le plus proche d'une maison personnelle en utilisant une fausse identité révélera immédiatement l'identité du client en tant que résident de la maison.

Comme nous avons vu dans le chapitre précédent que la vie privée est un problème majeur dans les affaires mobile. Parce que le client a la possibilité d'envoyer ses requêtes à tout moment et n'importe où. Dans ce chapitre, nous allons présenter et expliquer les mécanismes de préservation de la vie privée de localisation (LPPM) dans le m-business basé sur LBS. Ces mécanismes adoptent différents modèles, nous distinguons ainsi ceux qui sont basés sur la transformation géographique et ceux qui utilisent des modèles de collaboration.

En plus, nous allons présenter la classification des attaques sur la vie privée de client dans le m-business qui fournit les services de LBS.

3.2 Modèle de vie privée

Nous introduisons maintenant dans le système de m-business le problème de la vie privée de l'emplacement. Le problème de la protection de la vie privée se pose parce que les emplacements sont collectés par les fournisseurs de services LBS. La localisation représente des données personnelles alors que la collecte et l'utilisation de telles données sont donc soumises aux règles de vie privée.

Il existe une différence majeure entre les fournisseurs fiables (confiance) et non fiables. Les fournisseurs fiables doivent se conformer aux règlements sur la protection des renseignements personnels (par exemple, une société de cartes de crédit). Les fournisseurs non fiables sont ceux qui peuvent tenter de tirer profit du traitement des données personnelles sans le consentement de l'utilisateur, c.-à-d. les fournisseurs sont supposés être honnêtes mais curieux. Qu'un fournisseur soit digne de confiance ou non, dépendent de divers facteurs, notamment la réputation du parti [61]. La distinction entre les fournisseurs fiables et non fiables est au cœur des deux principales approches technologiques de la protection de la vie privée, qui ont été bien regroupées respectivement en concepts de vie privée souple et de vie privée stricte [62], où :

— Les solutions de vie privée ***souple*** s'appliquent lorsque le fournisseur est fiable. L'objectif est de veiller à ce que les utilisateurs sachent comment leurs renseignements personnels sont utilisés. Ces techniques complètent la notification légale du fournisseur.

— Les solutions de vie privée ***stricte*** s'appliquent lorsqu'au moins un des fournisseurs n'est pas fiable. Le but est de minimiser le transfert de données afin de réduire le besoin de confiance. Les solutions strictes tendent à automatiser ou à limiter considérablement l'intervention de l'utilisateur dans la configuration et la gestion de la vie privée.

On peut voir que la quantité de contrôle que les utilisateurs peuvent exercer est généralement différente pour les deux catégories de solutions. En plus, la vie privée stricte est alignée sur l'idée que la vie privée est une valeur en soi et doit être protégée indépendamment du contrôle que l'utilisateur peut exercer. Il n'existe aucune supériorité a priori d'une catégorie de solutions par rapport à une autre, c'est-à-dire que la commodité dépend du contexte de l'application [61].

Nous décrivons un modèle de protection de la vie privée en fonction des dimensions suivantes :

— ***Objectif de la vie privée*** : spécifie l'exigence de la vie privée de l'utilisateur.

— ***Mécanisme de protection de la vie privée*** : la technique utilisée pour atteindre l'objectif de la vie privée.

— ***Métrique de la vie privée*** : les critères de quantification du niveau de protection fourni par le mécanisme de protection de la vie privée.

Les objectifs de protection de la vie privée sont décrits ci-dessous (Section 3.5), tandis que les concepts de mécanisme de protection de la vie privée seront abordés dans Section 3.7.

3.3 Différentes structures du système de protection de la vie privée de client

Avant d'aborder les détails des différentes structures de système de protection de la vie privée, nous présentons un modèle de système commun qui correspond à la plupart des approches décrites dans la littérature.

3.3.1 Modèle de système commun

Ce modèle comprend trois composants, à savoir les périphériques utilisateur mobiles, un serveur central et les fournisseurs de services.

- ✓ **Dispositif mobile :** Le dispositif mobile d'un utilisateur est équipé d'un capteur de position intégré pour déterminer la position actuelle de l'utilisateur. Ce dispositif est supposé être de confiance, et il est garanti qu'aucun composant logiciel malveillant n'est en cours d'exécution sur l'appareil mobile qui a accès au capteur de position.
- ✓ **Serveur central :** Les appareils mobiles envoient leurs informations de position à un serveur central, qui stocke et gère les positions des appareils mobiles pour le compte de l'utilisateur. Le serveur central peut être non fiable ou fiable (digne de confiance). Dans le cas d'un serveur fiable, le serveur peut effectuer des calculs fiables et agir, par exemple, comme un serveur d'anonymisation (AS). En plus, un AS fiable peut utiliser un anonymiseur interne pour implémenter le concept de k-anonymat (Sect 3.4.1) en utilisant les positions de plusieurs utilisateurs mémorisées par le serveur AS pour rendre l'utilisateur impossible à distinguer de (k – 1) autres utilisateurs. De plus, le serveur AS peut calculer des positions masquées (caché) couvrant plusieurs utilisateurs.
- ✓ **Fournisseurs de services :** Les fournisseurs de services interrogent le serveur central pour connaître les positions des utilisateurs afin de mettre en œuvre un certain service basé sur la localisation. Le serveur central donne aux fournisseurs l'accès aux positions stockées sur la base d'un mécanisme de contrôle d'accès.

Le serveur central et les fournisseurs peuvent tous deux être compromis, même si ces entités sont supposées dignes de confiance. Par conséquent, nous considérons explicitement ce type d'attaque dans notre classification d'attaque (Sect 3.10.2.4). Si un serveur central est compromis avec succès par un attaquant, celui-ci est au courant de toutes les informations que les utilisateurs ont fournies au serveur central. Au contraire, un

fournisseur compromis n'a pas nécessairement accès à toutes les informations stockées au serveur central, mais seulement à une partie de celles-ci en fonction de ses droits d'accès.

Dans la littérature, il existe quelques types de structures de protection de la vie privée de client telles que structure de tiers de confiance (centralisé), structure distribuée et structure de pair à pair mobile.

3.3.2 Structure de tiers de confiance

L'idée principale de cette structure est d'utiliser un tiers de confiance, à placer entre les utilisateurs mobiles et le fournisseur de services LBS, appelé Anonymiseur Server (AS). Afin de répondre aux exigences de la vie privée de l'utilisateur, l'anonymiseur de la localisation AS est responsable de la confusion des emplacements d'utilisateur dans des régions cachées (camouflées) [14], [1], [63], [64], [65], [15] and [66]. Dans ce cas, les exigences de vie privée des utilisateurs sont généralement présentées en termes du modèle de K-anonymat, ce qui signifie que la région cachée contient au moins K utilisateurs, rendant chaque utilisateur impossible à distinguer parmi au moins K utilisateurs [67] et [45].

Il existe d'autres techniques d'anonymisation des emplacements utilisent cette approche d'architecture afin d'éviter le suivi des localisations (location tracking) de l'utilisateur pour les requêtes continues (les mises à jour continu des emplacements). Étant donné que le processeur de requêtes intégré dans le serveur de base de données (Fournisseur de services) ne connaît pas l'information de localisation réelle de la requête, il ne peut renvoyer qu'un ensemble de réponses incluant la réponse exacte à l'utilisateur, quel que soit son emplacement dans la région camouflée. Les structures de traitement de requêtes respectueuses de la vie privée existantes peuvent traiter des zones camouflées ***rectangulaires*** [68], [69], [15] and [70] ou ***circulaires*** [65] en tant que la requête et/ou des informations de localisation.

3.3.3 Structure distribuée

Dans ce modèle, les utilisateurs mobiles communiquent entre eux via une infrastructure de communication fixe, par exemple des stations de base [71] et [72]. L'idée de base des techniques d'anonymisation de l'emplacement dans cette architecture est que les utilisateurs collaborent avec d'autres pairs pour maintenir une structure de données distribuées où les informations de localisation stockées sont utilisées par les utilisateurs pour brouiller leurs informations de localisation dans les zones cachées basées sur le modèle K-anonymat. Ensuite, le traitement de la requête pourrait être similaire à celui utilisé dans l'architecture de tiers de confiance, où l'utilisateur envoie au serveur sa requête avec une zone masquée comprenant l'emplacement de l'utilisateur.

3.3.4 Structure de pair à pair mobile

Dans ce type, il n'y a pas d'infrastructure de communication fixe ni de serveurs centralisés / distribués. Au lieu de cela, les utilisateurs mobiles communiquent directement avec leurs pairs pour brouiller leurs emplacements dans des régions cachées qui satisfont à leurs exigences de vie privée comme K-anonymat personnalisé et/ou de région minimale [68]. Ensuite, le traitement de la requête pourrait être similaire à celui utilisé dans l'architecture de tiers de confiance. Lorsqu'un utilisateur trouve une région masquée comme son emplacement, il sélectionne au hasard un pair dans la région masquée en tant qu'agent. L'utilisateur envoie la requête avec la région masquée à l'agent, puis l'agent communique avec le fournisseur de services au nom de l'utilisateur. Lorsque l'agent reçoit un ensemble de réponses du fournisseur de services, il transmet la réponse à l'utilisateur. Enfin, l'utilisateur calcule la réponse exacte à partir de l'ensemble de réponses.

3.3.5 Comparaison des structures du système de protection de la vie privée du client

Dans le tableau 3.1, nous présentons une comparaison des structures du système de protection de la vie privée de client :

TABLE 3.1 – Comparaison des structures du système de protection de la vie privée [4].

Structure	Avantages	Inconvénients
Structure TTP	Facile à mettre en œuvre	La qualité du service dépend des performances du serveur central
Structure distribuée, Structure de pair à pair mobile	Pas besoin de serveurs tiers	La charge de travail de calcul du client est importante et l'effet de protection de la vie privée est faible.

Dans notre travail, nous nous intéressons à la structure de tiers de confiance TTP.

3.3.6 Informations échangées

Les informations échangées sont représentées par une requête. Cette dernière comporte deux caractéristiques principales : contenu et fréquence.

— ***Contenu*** : se compose souvent du temps d'émission de la requête, de l'identifiant et coordonnée géographique de l'utilisateur et d'autres informations supplémentaires (par exemple, le type de service). Il représente le noyau de la requête.

— ***Fréquence*** : décrit le nombre de demandes envoyées dans une période spécifiée. Les requêtes peuvent être échangées de façon ***Snapshots*** (sporadique) ou ***Continue***.

3.4 Concepts de base

k-anonymat et une tierce partie de confiance (TTP) sont les mêmes concepts de base utilisés par certaines approches. Cette section présente brièvement ces deux concepts :

3.4.1 k-anonymat

k-anonymat indique que dans un ensemble spécifique, un utilisateur est impossible à distinguer d'au moins k-1 autres utilisateurs. En d'autres termes, un ensemble est k-anonyme s'il inclut l'utilisateur et au moins k-1 autres utilisateurs identiques à lui en ce qui concerne les attributs considérés [73]. L'emplacement d'un utilisateur peut être représenté par un tuple contenant plusieurs dimensions : [x1, x2], [y1, y2] et [t1, t2]. Où, [x1, x2] et [y1, y2] décrivent la zone à deux dimensions dans laquelle l'utilisateur est positionné. Cette information est toujours nécessaire. De plus, la période de temps pendant laquelle l'utilisateur se trouvait dans la zone peut être déterminée par [t1, t2]. Le tuple ne donne pas les informations exactes de l'utilisateur, mais seulement une certaine plage lorsque $x1 \neq x2$, $y1 \neq y2$ et $t1 \neq t2$. Le tuple est k-anonyme lorsque la zone qu'il décrit englobe la position de l'utilisateur et au moins k-1 autres utilisateurs. Lorsqu'une approche s'appuie sur le k-anonymat ou sur des ensembles d'anonymat, il est important de noter que l'anonymat n'est fourni qu'en ce qui concerne l'information de localisation. D'autres informations spécifiques au service ou une connaissance préalable de l'adversaire pourraient encore identifier l'utilisateur [64].

3.4.2 Tierce partie de confiance (TTP)

Certaines des approches de protection de la vie privée supposent l'existence d'un tiers de confiance (TTP). Ce TTP est souvent appelé un serveur d'anonymisation (AS). Les utilisateurs d'un protocole d'anonymisation dans une zone souscrivent à l'AS. La tâche d'un **AS** est de recevoir l'emplacement fourni par l'utilisateur et à l'anonymiser conformément à l'approche sélectionnée. Il envoie ensuite la requête avec l'information traitée aux fournisseurs de services au nom de l'utilisateur et reçoit la réponse. Comme la réponse est adaptée pour fournir le service pour tous les points possibles dans la zone élargie et anonymisée, l'AS filtre la réponse. Il transmet ensuite la réponse exacte à l'utilisateur.

L'utilisation d'un AS pour assurer la vie privée de l'emplacement a été considérée de manière critique. L'AS est une autre tierce partie qui est utilisée, et l'étape la plus

difficile serait de trouver une instance digne de confiance. Construire une infrastructure de confiance AS nécessiterait beaucoup d'effort. De plus, le TTP est un point d'attaque unique pour un adversaire. En cas de compromission, l'attaquant récupère toutes les données, sans censure [74].

Un autre problème est que les algorithmes basés sur un TTP reposent sur d'autres utilisateurs utilisant le même AS. Ils doivent être présents dans la zone la plus proche pour pouvoir anonymiser correctement et pouvoir toujours fournir suffisamment d'informations. Même si le nombre requis d'utilisateurs existe, les informations de localisation que fournisseur reçoit ne seront jamais précises, mais constitueront toujours une zone agrandie. Cela peut entraîner une surcharge d'informations, car le serveur AS doit fournir des réponses pour tous les emplacements possibles compris dans la zone.

Mais l'utilisation d'un TTP apporte également un avantage à l'utilisateur : les calculs nécessaires au processus d'anonymisation ne sont pas effectués par l'utilisateur. L'utilisateur est soulagé des calculs lourds et d'autres détails liés aux algorithmes.

3.5 Objectifs de protection

Avant de discuter les différents mécanismes pour protéger la vie privée de l'utilisateur, dans cette section, nous définissons les différents objectifs de protection que ces mécanismes considèrent. Les attributs à protéger sont l'identité de l'utilisateur, ses informations spatiales (sa localisation) et ses informations temporelles (heure). Nous pouvons définir les informations fournies par un utilisateur comme un tuple (identité, la position et le temps).

L'objectif de la protection de la vie privée de l'utilisateur est de déterminer les attributs de l'information qui doivent être protégés et qui peuvent être révélés.

Tout d'abord, nous fournissons quelques exemples de différents objectifs de protection et scénarios d'application, avant d'examiner plus en détail la protection des attributs énoncés.

3.5.1 Exemples d'objectifs de protection

En tant que scénario d'application, considérons un utilisateur d'un système de m-business fournissant des services ou des informations de points d'intérêt en temps réel en fonction de la position actuelle de l'utilisateur. Nous supposons que l'utilisateur est prêt à fournir des informations de position anonymes au fournisseur de services. À cette fin, il protège l'attribut d'identité à l'aide d'un concept d'anonymisation. Cependant, comme décrit dans [75], l'identité de l'utilisateur peut également être révélée à partir des informations de localisation, par exemple sur la base des lieux de l'hébergement et du travail visités périodiquement. Par conséquent, l'attribut de position doit également être protégé.

Dans le deuxième scénario, supposons que l'utilisateur accepte de partager son chemin (piste) non anonyme. Cependant, il ne veut pas révéler qu'il roule trop vite sur l'autoroute car la divulgation de telles informations peut avoir un impact négatif sur l'utilisateur si le fournisseur de services abuse des données et les fournit à la police, à sa compagnie d'assurance, etc. Dans ce scénario, nous devons protéger les attributs de position et de temps pour empêcher le calcul de la vitesse maximale.

Pour atteindre les différents objectifs de protection, les différentes approches de la vie privée de l'emplacement sont nécessaires. Comme nous le verrons dans le prochain chapitre, aucune approche n'est adaptée pour protéger tous les objectifs de protection énoncés en même temps.

Dans ce qui suit, nous examinons plus en détail la protection de chaque attribut.

3.5.2 Identité de l'utilisateur

Un des objectifs possibles pour assurer la vie privée est de cacher l'identité de l'utilisateur pendant que la position de l'objet mobile anonyme est visible pour les fournisseurs de services. L'identité d'un utilisateur peut être son nom, un identifiant unique ou tout ensemble de propriétés identifiant l'utilisateur de manière unique. Si un utilisateur publie des informations de localisation sans informations personnelles, l'attaquant peut toujours tenter de dériver son identité en analysant les informations de localisation et des données de contexte supplémentaires telles que des objets visités. En général, les quasi-identificateurs peuvent être utilisés pour identifier l'utilisateur comme indiqué dans [51].

3.5.3 Information spatiale

L'autre objectif de la protection est de fournir au fournisseur des informations de localisation de l'utilisateur avec une précision spécifique. Par exemple, un utilisateur pourrait vouloir fournir des informations de localisation précises à ses amis, alors que seules les localisations qui ont délibérément détérioré la qualité de l'information sont fournies au fournisseur de services. En général, cet objectif est connu sous le nom d'obscurcissement de position ou de camouflage (Cloaking) [76].

Nous devons également considérer que la localisation d'un utilisateur contient généralement plus d'informations que des informations géométriques uniquement, telles que les valeurs de latitude et de longitude. Souvent, la sémantique de localisation définit la sensibilité des informations de la localisation. Par exemple, un utilisateur peut ne pas avoir de problème à partager une localisation particulière tant qu'il n'entre pas dans certains lieux sémantiques tels que les hôpitaux, où cela peut être utilisé pour dériver des informations privées telles que l'état de santé de l'utilisateur.

Par conséquent, l'objectif spécifique de la protection des informations spatiales est la protection de l'information de localisation sémantique. En général, ceci est réalisé en

s'assurant que la localisation est associée à de nombreux emplacements alternatifs de sémantique différente. Par exemple, une localisation sémantique peut être protégée si l'utilisateur est dans un hôpital ou dans un ou plusieurs lieux autres que des hôpitaux [77].

3.5.4 Informations temporelles

Les informations temporelles définissent le moment ou la période où les informations spatiales de l'utilisateur sont valides. Dans certains scénarios, les informations spatiales ne sont considérées comme critiques que si elles sont associées à des informations temporelles. Par exemple, un utilisateur pourrait être disposé à partager avec d'autres où il est en voyage, alors qu'il ne veut pas révéler qu'il est excès de vitesse. Cela signifie que les mises à jour ne peuvent pas être utilisées en temps réel sans causer de problèmes de la vie privée, tandis que les mises à jour différées peuvent être utilisées pour atteindre l'objectif de protection [2].

Dans de tels scénarios, il faut considérer que même si les informations temporelles ne sont pas explicitement indiquées (par exemple, comme horodatage (timestamp) de la mise à jour de la position), elles peuvent être implicitement dérivées. Par exemple, cela est possible en connaissant l'heure à laquelle les informations ont été reçues par le serveur d'anonymisation et en connaissant l'algorithme de mise à jour de la localisation qui a provoqué la mise à jour. En général, l'utilisateur peut vouloir contrôler la résolution temporelle de sa position ou de la trajectoire complète du mouvement [2].

3.6 Mesures technologiques pour la protection de la vie privée

De nombreuses mesures technologiques ont été avancées afin de résoudre les problèmes de protection de la vie privée associés aux services m-business basés sur l'emplacement (LBS). Certains de ces mécanismes offrent une protection complète des données personnelles, tandis que d'autres offrent une protection partielle, mais une combinaison de méthodes peut également être utilisée pour assurer le niveau de sécurité souhaité.

3.6.1 Protection de la vie privée par conception

Dans le contexte de m-business, la protection de la vie privée par conception signifie que les systèmes et les processus sont conçus pour recevoir seulement l'information nécessaire afin de traiter efficacement la requête de l'utilisateur. De plus, de tels processus peuvent retirer des identificateurs de l'information s'ils ne sont pas nécessaires au processus. De cette façon, un équilibre peut être maintenu entre les besoins du fournisseur de services et les intérêts de la vie privée des utilisateurs.

De plus en plus, la protection de la vie privée par conception est recommandée comme moyen par lequel les entreprises peuvent prendre des mesures pour intégrer les valeurs et les caractéristiques de la vie privée dans leurs produits et services. Bien que la protection de la vie privée par la conception ne soit pas une solution complète ou une solution nécessairement sans problèmes à la vie privée, la technologie peut offrir certaines options aux consommateurs.

3.6.2 Solutions existantes

Certaines entreprises intègrent des outils de gestion de la vie privée dans leurs dispositifs et services. Cela permet aux individus de gérer leurs données de localisation et de contrôler la quantité d'informations divulguées à des tiers. Par exemple, nous pouvons choisir de ne révéler que des informations de localisation générales, telles que le pays, ou de divulguer des détails supplémentaires, tels que la ville ou la rue. Ces mesures sont appropriées dans certains contextes. Par exemple, un code postal suffisant pour fournir à l'utilisateur une liste des restaurants Algériens de la région. Cependant, dans de nombreux cas, pour fournir un service véritablement interactif et pratique, l'utilisateur devrait divulguer plus que les données de localisation publiques.

La pseudonymisation est une technique utilisée pour protéger la vie privée. L'emplacement de l'utilisateur est associé à un pseudonyme, au lieu d'un nom réel. Cependant, cette méthode s'est révélée imparfaite, car il est rapidement devenu évident que d'autres informations d'identification (telles que le domicile ou le lieu de travail de l'utilisateur) pourraient facilement être distinguées avec des connaissances antérieur (background) sur l'utilisateur [78].

Des alternatives à la pseudonymisation ont été recherchées et avancées au cours des dernières années. Leur objectif principal est de trouver des moyens de protéger l'association entre l'utilisateur et ses renseignements personnels qui pourraient mener à une ré-identification [79].

Dans la littérature, il existe plusieurs des mécanismes de protection de la vie privée, nous distinguons deux types de modèles utilisés dans ces mécanismes. Il y a des mécanismes basés sur les modèles de transformation géographique et d'autres mécanismes utilisent les modèles de collaboration.

3.6.2.1 Modèles de transformation

Les modèles de transformation incluent des techniques qui effectuent des opérations géographiques sur les coordonnées d'un utilisateur afin de protéger leurs emplacements physiques (réels) [80].

Pour préserver la vie privée, l'emplacement exact des utilisateurs qui envoient des requêtes aux fournisseurs LBS ne doit pas être divulgué. Au lieu de cela, les données de localisation sont d'abord perturbées ou cryptées. Par exemple, certaines tech-

niques existantes génèrent quelques des endroits fictifs aléatoires et d'envoyer un certain nombre de requêtes redondantes aux fournisseurs pour empêcher l'identification des utilisateurs [81], [82].

La réalisation de la vie privée impose des coûts supplémentaires lors du traitement des requêtes, par exemple, il convient de traiter un plus grand nombre de requêtes dans le cas de techniques générant des requêtes redondantes. Le traitement des requêtes dans les techniques de k-anonymat est effectué par rapport à la région de camouflage, ce qui est considérablement plus coûteux que les requêtes ponctuelles. Par conséquent, un compromis se crée entre la vie privée et la performance [83].

Nous pouvons classer les techniques de transformation spatiales existantes préservant la vie privée en deux catégories, en fonction de l'architecture qu'elles adoptent :

- ✓ ***Transformations spatiales à deux niveaux*** dans cette catégorie, les méthodes ne nécessitent aucune tierce partie de confiance et l'anonymisation de la requête est effectuée par l'utilisateur mobile lui-même.
- ✓ ***Transformations spatiales à trois niveaux*** les méthodes de cette catégorie supposent la présence un tiers de confiance, ***a trusted third-party TTP***, (comme un serveur d'anonymisation) et offrent une meilleure protection contre les attaques de connaissances antérieur (***background knowledge attacks***) par exemple, un attaquant peut avoir des informations supplémentaires sur les emplacements des utilisateurs, à partir d'une source externe.

Le compromis (The trade-off) est que les méthodes de la deuxième catégorie génèrent davantage de temps d'exécution, car elles obligent les utilisateurs à mettre à jour de manière coûteuse leur emplacement avec une autorité centrale, et les algorithmes utilisés pour générer des régions de protection masquées sont plus coûteux en termes de calcul.

3.6.2.2 Modèles de collaboration

Les mécanismes de deuxième type utilisent la collaboration entre les utilisateurs du même système de m-business, et ils peuvent ne pas se baser sur une transformation des coordonnées géographiques. En plus, les mécanismes de collaboration garantissent la participation des utilisateurs, et ils peuvent non seulement fournir de solides garanties de vie privée, mais ils sont également plus susceptibles d'être adopté par les utilisateurs [84].

Bien que de nombreux mécanismes de coopération aient été proposés [85], [86] et [87], la plupart d'entre eux se basent sur les mécanismes de transformation.

3.7 Mécanismes de protection de vie privée

Après avoir présenté les objectifs de la vie privée possibles dans la présente section 3.5, nous donnons un aperçu des mécanismes existant de protection de la vie privée de l'utilisateur pour atteindre ces objectifs.

Le mécanisme de protection de la vie privée est la technique utilisée pour atteindre l'objectif de protection de la vie privée. De manière abstraite, il peut être défini comme une transformation qui mappe la requête de chaque utilisateur dans une requête différente avant qu'elle ne devienne observable pour l'adversaire [61]. Dans le cas le plus général, la transformation consiste en deux fonctions, la première pour transformer l'identité de l'utilisateur en un pseudonyme basé sur certains critères (si l'utilisateur doit être anonyme) et la seconde pour transformer l'emplacement [88].

La vie privée dans m-business fournissant LBS dépend de deux facteurs principaux : la protection des données sensibles des utilisateurs dans la requête et intraçabilité (la non-liaison) entre la localisation de l'utilisateur et la requête. Par conséquent, nous avons classé la vie privée de l'utilisateur de m-business en deux types : la vie privée de localisation et la vie privée de la requête.

Il y a un certain nombre d'œuvres représentant l'état de l'art des mécanismes pour protéger la vie privée de localisation. Le but de cette section est donc de donner un aperçu des principes fondamentaux de ces mécanismes.

3.7.1 Protection de la vie privée de la localisation (Location privacy)

En général, les mécanismes de protection peuvent être vus selon deux composants principaux : Le modèle utilisé dans LPPM (Location Privacy-Preserving Mechanism) pour atteindre les objectifs souhaités de la vie privée et les mesures utilisées pour évaluer son efficacité par rapport à un ensemble prédéfini d'exigences de confidentialité.

Plusieurs études ont montré que la séparation entre les données de localisation d'un utilisateur et ses informations d'identification peut être obtenue grâce à des méthodes technologiques de protection des données telles que l'anonymisation d'emplacement, les techniques cryptographiques, l'obscurcissement ou d'autres. Basé sur les principes de la vie privée, et les problématiques majeures liées à l'utilisation de m-business, plusieurs travaux ont été proposés afin de permettre aux utilisateurs de préserver leur vie privée de la localisation tout en profitant les services de localisation [89], [90], [91], [92].

Dans les sous sections ci-dessous, nous présentons un ensemble varié des mécanismes les plus modernes et les plus couramment utilisées :

3.7.1.1 Obscurcissement et perturbation de la localisation

Les mécanismes d'obscurcissement de localisation utilisent la transformation des coordonnées géographiques pour masquer ou camoufler l'emplacement réel de l'utilisateur dans une zone géographique plus large. Le but principal de l'obscurcissement de localisation est de dégrader délibérément la qualité de l'information de la localisation d'un utilisateur afin de protéger son intimité (vie privée) de localisation [63]. En plus, ces mécanismes perturbent les informations de localisation réelles tout en maintenant une liaison avec les identités des utilisateurs (c.-à-d. modifier ou déplacer de sa position d'origine).

L'idée de ce mécanisme est d'utiliser un journal des emplacements historiques des utilisateurs plutôt que l'information sur l'emplacement en temps réel pour générer des régions de camouflages (masquées ou obscurcies) [93], [94]. En outre, il utilise k-anonymat comme métrique pour mesurer la vie privée de l'emplacement de l'utilisateur.

M. Duckham et al [63] présentent la définition officielle de l'obscurcissement de la localisation peut être "le moyen de dégrader délibérément la qualité des informations sur la localisation d'une personne afin de protéger la vie privée de cette localisation".

En d'autres termes, l'obscurcissement de localisation vise à représenter l'emplacement réel de l'utilisateur lu sur une région plus grande R (la région de camouflage) qui doit nécessairement contenir l'emplacement lu Figure 3.1. L'approche classique d'obscurcissement spatial est celle présentée par Ardagna et al [76], où un utilisateur envoie au serveur central une zone circulaire au lieu de la localisation exacte de l'utilisateur.

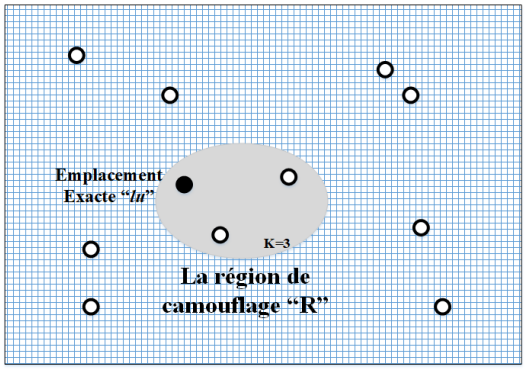


FIGURE 3.1 – Exemple de obscurcissement.

Ce mécanisme est largement utilisé dans différentes LPPM. Bien que certaines applications l'adoptent pour protéger les coordonnées exactes de l'utilisateur [95], [96]. En plus, il existe d'autres applications qui utilisent des mécanismes basés sur l'obscurcissement pour éviter de divulguer la trajectoire et le comportement de l'utilisateur [97], [98], ou pour se protéger contre la ré-identification [64], [65].

L'avantage des approches d'obscurcissement spatial réside dans le fait qu'elles fournissent une vie privée de localisation sans TTP, où l'utilisateur peut identifier lui-même la zone d'obscurcissement [2]. Cependant, les fournisseurs de services ne disposent pas

d'un emplacement exact d'utilisateur. Ce compromis (trade-off) entre la vie privée et la précision a été étudié par Cheng et al [99].

Pour appliquer le concept d'obscurcissement de la localisation aux réseaux routiers, Duckham et Kulik [63] utilisent des graphes d'obscurcissement au lieu d'utiliser des formes d'obscurcissement géométriques telles que des cercles. Gutscher et al [100] proposent une approche basée sur la transformation des coordonnées. Les utilisateurs mobiles effectuent quelques opérations géométriques simples (déplacement, rotation) sur leurs positions avant de les envoyer au serveur central.

Dans [101], Hashem et al présentent une approche basée sur le groupe d'utilisateurs. Cette approche protège la vie privée de la localisation des utilisateurs en fournissant des régions au lieu de positions précises dans la requête K-NN du groupe à fournisseur de services.

Un problème avec de nombreuses techniques d'obscurcissement spatiales est que la taille effective de la zone d'obscurcissement destinée peut être réduite si un adversaire applique les connaissances antérieures, en particulier, la connaissance de la carte.

3.7.1.2 Dummies (mannequins)

Une solution pour atteindre l'anonymat de localisation sans avoir besoin d'un TTP est la création de requêtes factices. L'utilisateur ne demande pas seulement le service fourni pour un, mais pour de nombreux emplacements. En plus, seul l'utilisateur doit connaître l'emplacement réel [102].

L'objectif principal des Dummies est de sécuriser la vraie localisation d'un utilisateur, autrement dit, le mécanisme qui utilise le modèle de Dummies transmet la localisation réelle de l'utilisateur avec un groupe d'autres localisations factices (Dummies) au fournisseur de services pour le cacher. Dans cette technique, les fournisseurs de services renvoient des résultats basés sur la localisation pour chaque position du groupe reçu. Ensuite, les résultats correspondant à la localisation réelle de l'utilisateur sont extraits de l'ensemble des résultats. Ce mécanisme utilise métrique k-anonymat pour mesurer la vie privée de la localisation des utilisateurs.

Le principal avantage de cette approche est que l'utilisateur lui-même peut générer des Dummies (requêtes factices) sans la nécessité d'un tiers TTP. Cependant, cette approche peut réduire la facilité d'utilisation des données réelles par rapport aux données factices (Dummy data) [103].

Toutefois, il serait facile de comprendre les requêtes factices lorsque l'adversaire dispose d'informations contextuelles supplémentaires telles qu'une carte, surveille l'utilisateur sur une plus longue période de temps ou vérifie les emplacements pour la validité (un emplacement au milieu d'un lac semble peu probable d'être la position réelle dans la plupart des cas). Par conséquent, les requêtes factices doivent être construites avec soin [104].

C'est pour cela, il est difficile de créer des Dummies qui ne peuvent pas être distinguées de l'emplacement réel de l'utilisateur.

L'approche SybilQuery suggérée par Shankar et al [74] suppose que l'utilisateur dispose d'une base de données de trafic historique lui permettant de créer des localisations factices supplémentaires qui ne peuvent pas être distinguées de son emplacement réel.

Même lorsque cette approche peut assurer la vie privée et l'utilité, une grande quantité de bruit pouvant être ajoutée aux données de localisation peut compromettre d'autres aspects de l'utilité.

3.7.1.3 mix-zones

Le mécanisme de mix-zones est proposé par Beresford et al [105]. L'idée de cette mécanisme est de définir des zones appelées zones de mixage, dans lesquelles tous les emplacements d'utilisateurs doivent être masquées afin que l'emplacement de l'utilisateur ne soit pas connu dans ces zones. Ceci est réalisé par aucun utilisateur n'envoyant de mises à jour d'emplacement dans la zone. En plus, les auteurs supposent que chaque utilisateur doit avoir au moins une région géographique dans laquelle les fournisseurs ne peuvent pas récupérer son emplacement.

L'idée principale de ce mécanisme est de modifier les pseudonymes des utilisateurs afin de protéger les identités des utilisateurs, c.-à-d., si un utilisateur entre dans une zone de mixage, l'identité de l'utilisateur est mélangée avec tous les autres utilisateurs de la zone. Ainsi, l'attaquant ne peut pas relier différents pseudonymes des utilisateurs, même en traçant des points d'entrée et de sortie dans la zone de mixage.

Cette technique convient aux services qui suivent en permanence le mouvement des utilisateurs dans les applications de m-business. Cela dépend de la transformation géométrique de l'emplacement et utilise des mesures de vie privée pour mesurer le niveau de vie privée de l'emplacement.

Palanisamy et Liu [106] proposent l'approche de MobiMix, où les auteurs appliquent le concept de mix-zones aux réseaux routiers. Ils prennent en compte différentes informations de contexte pouvant être utilisées par un attaquant pour extraire des trajectoires détaillées telles que des contraintes géométriques et temporelles.

3.7.1.4 Cloaking (camouflage)

k-anonymat est un concept répandu de la vie privée générale et ne se limite pas à la vie privée de l'emplacement. Gruteser et Grunwald [64] ont introduit le concept de k-anonymat pour la vie privée de la localisation. Ainsi, k-anonymat garantit que dans un ensemble de k clients mobiles, l'émetteur de requête ne peut pas être distingué des k-1 autres clients. Par conséquent, la probabilité d'identifier l'émetteur de requête est 1 / k.

L'idée principale de ce mécanisme est qu'un utilisateur signale à un fournisseur de

services une région de camouflage (cloaked region) contenant sa localisation exacte et les localisations d'au moins k autres utilisateurs au lieu de sa localisation précise protégée par un pseudonyme. Ici, le serveur (AS) agit comme un serveur TTP pour calculer l'ensemble des k utilisateurs et la région de camouflage en fonction de ses localisations d'utilisateur connues [2]. Avec le cloaking, le fournisseur de services ne recevra jamais les informations exactes, mais seulement un certain intervalle dans lequel les informations de localisation vraies sont incluses [104].

Par exemple, supposons qu'Alice se trouve actuellement à la maison et interroge un service de localisation, par exemple, la clinique de cardiologie la plus proche. Sans l'utilisation de la dissimulation d'identité, cette requête peut révéler au fournisseur qu'Alice rencontre des problèmes de santé. En utilisant k-anonymat, il serait impossible de distinguer Alice d'au moins k-1 autres utilisateurs, de sorte que le fournisseur ne puisse pas lier la demande à Alice. Par conséquent, il est essentiel que tous les k utilisateurs (l'ensemble d'anonymisation calculé envoyé au fournisseur) partagent la même région de camouflage (d'obscurcissement), afin que le fournisseur ne puisse pas lier la localisation émise à l'emplacement de la maison d'Alice [2].

Dans certaines implémentations, l'utilisateur peut être en mesure de spécifier le paramètre k. Dans bon nombre de ces techniques, on utilise des régions camouflées pour fournir un tel anonymat, où les k utilisateurs sont assez semblables à l'intérieur d'une région, pour tromper les attaquants en les empêchant d'identifier l'émetteur réel d'une requête, de sorte que les régions camouflées sont plus petites dans les zones où la densité d'utilisateurs est plus élevée [8].

Gruteser et Grunwald [64] distinguent les différents domaines d'application en fonction de leurs besoins d'informations spatiales ou temporelles exactes :

— ***Cloaking Spatiale*** : L'idée de cloaking spatial consiste à calculer une région dite région de camouflage englobant l'utilisateur et au moins (k-1) autres utilisateurs. Cette région de camouflage est ensuite transmise aux fournisseurs de services. Une option pour implémenter le camouflage spatial est un algorithme basé sur Quadtree [64]. L'algorithme est fourni avec les informations de l'utilisateur, le paramètre kmin, qui détermine la taille minimale de l'ensemble d'anonymat, la zone couverte par l'anonymiseur et les informations de tous les autres utilisateurs dans la région. En résumé, l'algorithme coupe la zone considérée tant qu'il y a au moins k - 1 autres utilisateurs dans la même zone que l'utilisateur. Le plus petit quadrant qui remplit encore cette contrainte est alors renvoyé.

— ***Cloaking temporelle (camouflage temporel)*** : Si une information spatiale plus exacte pour un service est nécessaire, on peut utiliser le camouflage temporel, où la précision temporelle est réduite. Comme tous les utilisateurs sont présents dans la région dans un certain intervalle de temps et pas seulement à un moment donné, le nombre d'utilisateurs disponibles pour l'anonymisation augmente. Pour

le camouflage temporel, la demande de l'utilisateur est retardée jusqu'à ce que k d'autres utilisateurs aient résidé dans la zone déterminée par un paramètre de résolution. Le paramètre de résolution détermine le degré d'inexactitude des informations d'emplacement (Amin). La plage de temps $[t_1, t_2]$ est ensuite calculée comme suit : t_2 est l'heure actuelle, t_1 l'heure de la demande de l'utilisateur moins un facteur de cloaking aléatoire. Le tuple contenant les informations spatiales et temporelles est ensuite renvoyé.

3.7.1.5 Approches basées sur la cryptographie

Afin de protéger les localisations des utilisateurs, les approches de vie privée de localisation cryptographique utilisent le chiffrement. Mascetti et al [107] proposent une approche pour informer les utilisateurs lorsque des amis se trouvent à proximité sans révéler la localisation actuelle de l'utilisateur à fournisseur de LBS. À cette fin, les auteurs utilisent des techniques de cryptage symétrique et supposent que chaque utilisateur partage un secret avec chacun de ses amis. Ghinita et al [95] suggèrent une autre approche pour assurer la vie privée de l'emplacement grâce à l'utilisation de la technique de recherche d'informations personnelles (PIR). Le fournisseur des services peut répondre à des requêtes sans apprendre ou révéler des informations de la requête par utilisation de PIR.

3.7.2 Protection de la vie privée de requête (Query Privacy)

Il existe des approches basées sur le chiffrement pour interroger les serveurs non fiables comme symétrique, asymétrique [108] ou [109]. Les nœuds de chiffrement des clés asymétriques sont relativement plus coûteux comparativement au chiffrement symétrique des clés, peuvent être utilisés pour l'interrogation des emplacements dans des applications sociales basées sur l'emplacement comme par exemple ***Locx*** [110].

3.8 Évaluation

Compte tenu de l'existence de divers mécanismes pour protéger la vie privée des localisations, il n'est pas possible de fournir une évaluation quantitative de toutes ces solutions dans un scénario commun et d'indiquer qu'un seul mécanisme est le meilleur pour toutes les situations. Dans cette section, nous allons proposer une comparaison qualitative des mécanismes à partir d'un tableau de comparaison simple. Le tableau 3.2 fournit un bon aperçu de la nature de nombreux LPPM existants, qui devraient devenir notre guide afin de sélectionner le mécanisme qui offre les meilleures caractéristiques pour nos besoins [8]. Afin de fournir au moins un outil initial pour comparer les mécanismes de LPPM, certains facteurs clés sont proposés [8] :

- ✓ Nécessite un tiers de confiance ou d'un composant matériel de confiance.
- ✓ Signale toute information de localisation au Fournisseur de services.
- ✓ Nécessite une implémentation spéciale du côté fournisseur de services.
- ✓ Efficacité (la vie privée et utilité).
- ✓ Types de requêtes : Snapshots ou Continues.

Le fait d'avoir un tiers puissant (comme le serveur AS) peut fournir au système de m-business un certain niveau de sécurité que le système distribué ne peut pas atteindre, tel que la vérification de l'identité.

Comme il existe déjà de nombreuses applications, par conséquent, pour inclure le mécanisme, des implémentations spéciales du côté du fournisseur de services peuvent nécessiter un investissement important. Pour cela, la solution LPPM nécessitait probablement juste des changements au niveau de l'application client, et un investissement minimal ou nul investissement du côté fournisseur [8].

TABLE 3.2 – Récapitulatif des modèles de protection de la vie privée de localisation.

Mécanismes	Propriétés						
	Nécessite un tiers de confiance	**Signale toute information de localisation au Fournisseur de services**	**Snapshots**	**Continue**	**Vie privée**	**utilité**	**Nécessite une implémentation spéciale**
Obscurcissement de la localisation, K-Anonymat et Cloaking Spatial	Non	Région	Oui	Oui	Oui	Oui	Non
Localisation des Dummies	Non	Oui	Oui	Non	Oui	Non	Non
Mix-zones	Oui	Oui	Oui	Non	Oui	Non	Non
Cryptographie	Non	Non	Oui	Oui	Oui	Non	Oui

3.9 Discutions et Analyse

La protection de la vie privée est réalisée avec une surcharge supplémentaire en termes de coûts de calcul et de communication.

De plus, en termes de périphériques spéciaux, cela augmenterait les coûts d'une implémentation réelle, mais dans certains cas, cela peut devenir nécessaire, comme lorsque le matériel à usage général est vulnérable et que l'application est utilisée dans des environnements critiques, comme dans des scénarios militaires où la communication cryptographique câblée peut être nécessaire pour éviter l'écoute de la part de l'ennemi.

Savoir si l'application doit déclarer informations sur l'emplacement est un facteur important doit être à prendre en compte. Idéalement, l'emplacement exact ne soit pas partagé mais uniquement lorsque cela est nécessaire.

Les techniques cryptographiques et celles qui déclarent des régions plutôt que des emplacements seraient souhaitables pour les applications critiques, comparativement aux techniques dans lesquelles l'emplacement est partagé, même s'il est légèrement modifié.

D'autre part, pour les applications non critiques qui peuvent ne pas être très importantes de révéler l'emplacement, le coût des techniques cryptographiques peut être élevé en termes d'accès aux informations réelles et du type de services fournit par rapport aux données légèrement modifiées ou codées. Par rapport à une technique telle que l'obscurcissement ponctuel qui peut offrir un certain niveau de protection à faible coût, tout en préservant la validité géographique des données et leur disponibilité pour une utilisation immédiate. Les méthodes géométriques et cryptographiques fournissent divers compromis entre la vie privée et la performance [83].

3.9.1 Aspect de la vie privée

Les régions de camouflages des approches de transformations spatiales empêchent la ré-identification de l'utilisateur, car elles contiennent au mois k utilisateurs réels. Néanmoins, la région de camouflage dans le pire des cas peut dégénérer jusqu'à un certain point, pour cela elle peut avoir une étendue réduite. Par conséquent, un attaquant peut apprendre où se trouve la source de la requête (et un certain nombre de k-1 autres utilisateurs), et associer les emplacements de tous les utilisateurs dans la région de camouflage avec une fonctionnalité sensible, mettre ainsi leur vie privée en danger [83].

La formation de requêtes à l'aide d'une approche cryptographique est plus adaptée à la préservation de la vie privée. Ainsi, la méthode PIR décrite dans [111] fournit une protection complète de la vie privée dans tous les modèles d'attaque, où aucune information de localisation d'utilisateur n'est divulguée. Par conséquent, aucune association ne peut être établie entre les utilisateurs et les emplacements sensibles. Même dans le

cas où l'attaquant connaît l'emplacement exact de tous les utilisateurs, l'association entre les utilisateurs et les requêtes est encore empêchée. Les garanties de vie privée s'appliquent également aux requêtes continues (les utilisateurs en mouvement) [83].

3.9.2 Aspect de la performance

Les traitements de requêtes redondantes sont les principaux frais généraux encourus par l'approche de la génération des Dummies. Cependant, il n'y a qu'un seul cycle de traitement.

Les méthodes d'anonymat spatial entraînent une surcharge en termes de traitement de requête, où une requête de région est traitée dans une région de camouflage.

Les opérations cryptographiques peuvent entraîner des coûts plus élevés de traitement de requête et les frais généraux de calcul et de communication sur les serveurs [103]. En général, les approches cryptographiques soulèvent la question de savoir si les requêtes basées sur l'emplacement peuvent être exécutées efficacement au moyen des données cryptées, quels que soient les types de requête (nearest-neighbor-queries ou range queries). La figure 3.2 présente une représentation graphique des approches présentées en ce qui concerne le compromis obtenu entre le respect de la vie privée et la performance obtenue [83].

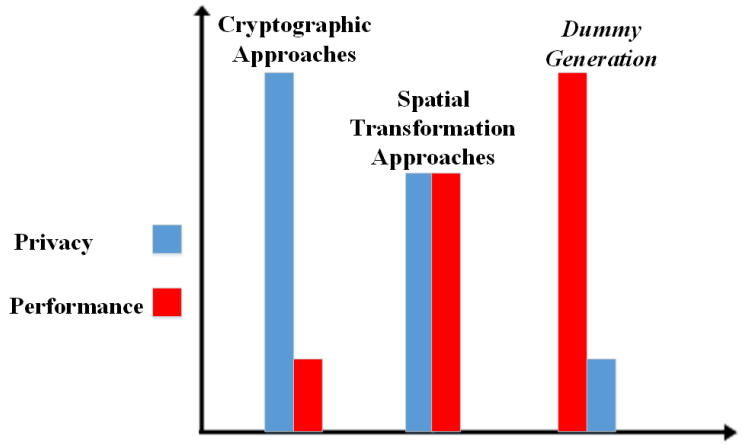


FIGURE 3.2 – Compromis entre la performance et la protection de la vie privée.

3.10 Classification des attaques contre la vie privée de client

La représentation de l'adversaire dépend de deux facteurs principaux : les connaissances antérieures et les attaques qu'il peut réaliser ainsi que la probabilité de leur succès.

Par conséquent, dans cette section, nous classons différentes attaques contre la vie privée des localisations, mais avant cela, nous présentons d'abord une classification des attaquants en fonction de leurs connaissances antérieures qu'ils exploitent pour dériver des informations privées.

3.10.1 Connaissance antérieures de l'attaquant

Les auteurs de [2] classent les connaissances antérieures de l'attaquant selon deux dimensions, à savoir l'information temporelle et l'information contextuelle (voir la figure 3.3).

3.10.1.1 Dimension temporelle

Dans la dimension temporelle, nous examinons si un attaquant a seulement accès à une position utilisateur unique ou si l'attaquant peut accéder à l'information historique. Dans le premier cas, l'attaquant ne connaît qu'un seul instantané d'une position utilisateur (snapshot query). Cette hypothèse est commune pour de nombreuses approches de la vie privée.

Dans le second cas, l'attaquant connaît un ensemble de mises à jour pour plusieurs emplacements collectés au fil du temps, voire une trajectoire de mouvement entière. Ces informations peuvent être révélées, par exemple, par un Serveur central compromis ou Fournisseur compromis. En particulier, l'attaquant pourrait également obtenir des informations historiques de position de plusieurs utilisateurs, si un Serveur central a été compromis [2].

3.10.1.2 Dimension de contexte

Dans la dimension contextuelle, nous déterminons si l'adversaire dispose des informations supplémentaires au-delà de l'information spatiales et temporelles. En effet, un attaquant pourrait utiliser ces informations en les corrélant avec des positions connues de l'utilisateur. Parce que ces informations (telles que, un annuaire téléphonique et une carte) peuvent fournir des informations contextuelles supplémentaires à l'attaquant. Par exemple, un attaquant pourrait réduire la taille de la zone d'obscurcissement d'un utilisateur en utilisant la carte du réseau routier pour déterminer où les utilisateurs peuvent se déplacer, ou en utilisant l'annuaire pour spécifier l'adresse de domicile d'un utilisateur [80].

En pratique, la plupart des mécanismes existants ne prennent en compte que le cas où l'adversaire n'accède qu'à une seule position. Cependant, la majorité des applications de m-business reflètent la situation dans laquelle l'adversaire accède à un ensemble des positions, parfois des trajectoires. En fait, les services de m-business enregistrent toutes les requêtes reçues, qui sont formées en accumulant des connaissances antérieures

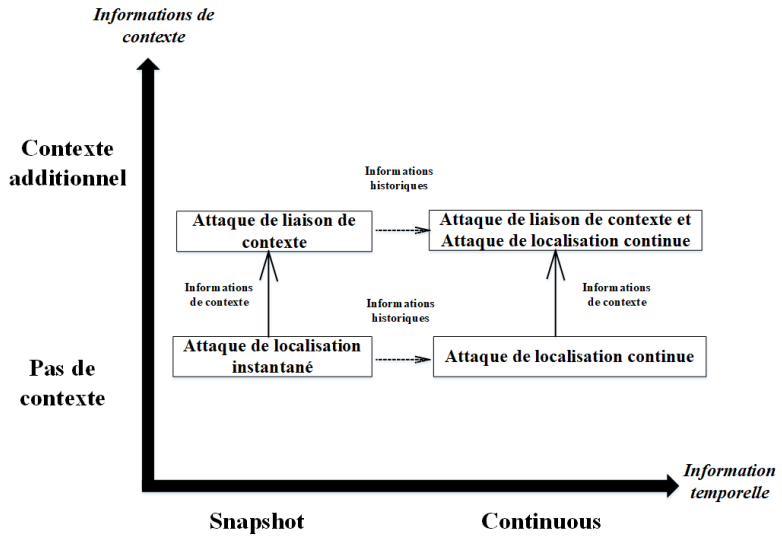


FIGURE 3.3 – Classification des connaissances de l'attaquant.

contenant des localisations, des trajectoires et des requêtes basées sur la localisation (Location-based queries).

L'efficacité du modèle d'adversaire dépend non seulement des connaissances antérieures ou l'information observée, mais également de l'efficacité des techniques et des mécanismes d'attaques utilisées. Nous discutons ci-dessous des principales techniques d'attaque et de leur applicabilité dans notre contexte.

3.10.2 Modèles d'attaque de la vie privée

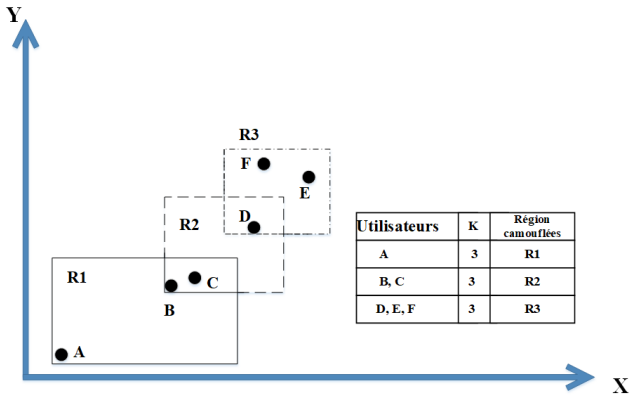
Nous distinguons entre Snapshot location attack, Continuous location attack, les attaques de contextualisation et les attaques basées sur la compromission d'un composant TTP.

3.10.2.1 Attaque d'emplacement instantané (*Snapshot location attack*)

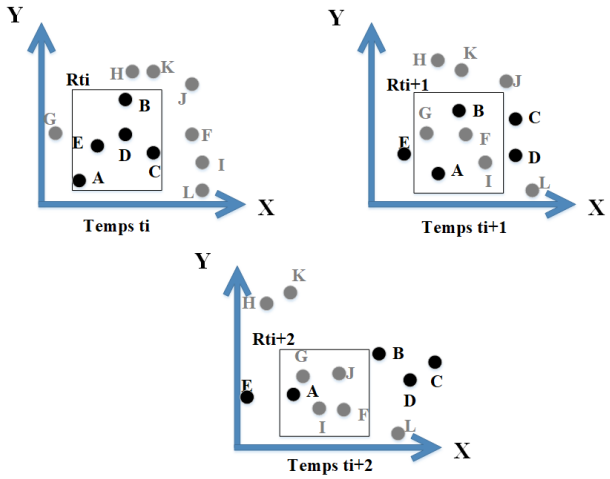
L'idée générale de ce type d'attaque est que l'attaquant analyse une requête unique pour obtenir plus d'informations sur l'utilisateur comme l'emplacement ou l'identité que l'utilisateur souhaite masquer. Certains types d'attaques peuvent se produire lorsque les emplacements d'instantanés exacts sont divulgués :

1. ***Location linking attack :*** Les informations de localisation contenues dans une requête utilisateur sont utilisées comme quasi-identifiant pour ré-identifier l'utilisateur [112], [52], [113], [45]. Par exemple, la requête peut être liée au propriétaire de l'emplacement, si un emplacement appartient exclusivement à un propriétaire. Le modèle de k-anonymat a été proposé pour prévenir ce type d'attaque [64]. Les auteurs de [64] proposent un algorithme de cloaking Quad-Tree pour générer des régions masquées.

2. ***Query sampling attacks :*** Les adversaires peuvent utiliser ce modèle d'attaque de la vie privée pour lier les utilisateurs avec les emplacements révélés à leurs requêtes. En plus, si les informations de localisation de l'utilisateur dans une zone clairsemée sont connues, alors, en utilisant l'attaque d'échantillonnage de la requête, un adversaire peut lier cet emplacement à une certaine requête [1]. Même si les emplacements sont masqués, un adversaire peut toujours être en mesure de lier une requête à son utilisateur dans le cas où les emplacements de l'utilisateur sont connus publiquement (l'association entre les utilisateurs et les requêtes) [10].



(a) Attaques d'échantillonnage de requêtes



(b) Attaque de tracking des requêtes

FIGURE 3.4 – Modèles d'attaque de la vie privée [1].

Scénario d'attaque :; supposons qu'il existe trois requêtes Q_{U1}, Q_{U2} et Q_{U3} sont envoyées par trois utilisateurs U1, U2 et U3, respectivement. Supposons que k=2. Selon le modèle k-anonymat, l'utilisateur U1 pourrait être caché dans une région R_1 qui couvre U1 et U2, et les utilisateurs U2 et U3 pourraient être cachés dans une autre région R_2 qui couvre les deux. Ensuite, un adversaire peut déduire que QU1 doit être émise par U1 puisque seul QU1 est avec R1 et seulement U1

doit être couvert par R_1 (U2 peut être couvert par R_1 ou R_2). Ce genre d'attaques sont appelées ***attaques d'échantillonnage de requêtes*** [1].

Autre scénario : comme le montre la figure 3.4 (a), qui représente un exemple d'une ***attaque d'échantillonnage de la requête*** où il y a six utilisateurs A, B, C, D, E et F. Comme la plupart des techniques de camouflage spatiales existantes ne font pas de distinction entre la vie privée de l'emplacement et la vie privée des requêtes, les utilisateurs ne peuvent fournir qu'une seule valeur pour k-anonymat (k=3). Le résultat de camouflage est que l'utilisateur A a R_1 comme région camouflée, les utilisateurs B et C ont R_2 comme région camouflée, tandis que les utilisateurs D, E et F ont R_3 comme région camouflée. Dans le cas où les emplacements des utilisateurs sont connus publiquement, un adversaire peut voir que l'utilisateur A est un utilisateur aberrant pour le système. Ensuite, l'adversaire peut déduire que la requête est envoyée par l'utilisateur A situé dans la zone clairsemée, à partir de la région camouflée R_1. L'idée principale est que si la requête a été émise par un autre utilisateur, la région spatiale camouflée doit d'abord couvrir les utilisateurs environnants dans la zone dense pour générer une région spatiale camouflée plus petite. Par conséquent, compte tenu de la connaissance de l'emplacement de l'utilisateur, un adversaire peut lier les requêtes basées sur l'emplacement à ses utilisateurs.

Pour faire face à de telles attaques (query sampling attacks, location linking attacks), les auteurs [1] ont suggéré d'employer des régions de k-sharing, c.-à-d., une région camouflée devrait également partager par au moins k de ses utilisateurs, non seulement couvrir au moins k de ces utilisateurs.

3. ***Attaque d'homogénéité de localisation*** L'attaque d'homogénéité peut être utilisé contre les approches simples qui se basent sur le modèle de k-anonymat, puis que l'attaquant peut analyser les positions de tous les utilisateurs du k-cluster. Par conséquent, les informations de localisation sont révélées pour chaque utilisateur si leurs localisations sont presque identiques (comme illustrée dans la figure 3.5 (a)).

   Les informations de localisations sont protégées si les utilisateurs du cluster sont répartis sur une région plus étendue (voir la figure 3.5 (b)). L'utilisation des connaissances cartographiques par l'adversaire réduit la taille effective de la région où les utilisateurs peuvent être localisés. Par exemple, la région peut être limitée à un seul bâtiment (voir la figure 3.5 (c)). Ici, l'attaquant analyse les informations de la localisation sémantique pour les utilisateurs du cluster et détermine la diversité des informations de localisation. Par conséquent, les informations de position homogènes ne garantissent pas la vie privée de l'emplacement, contrairement aux informations de position diverses [114].

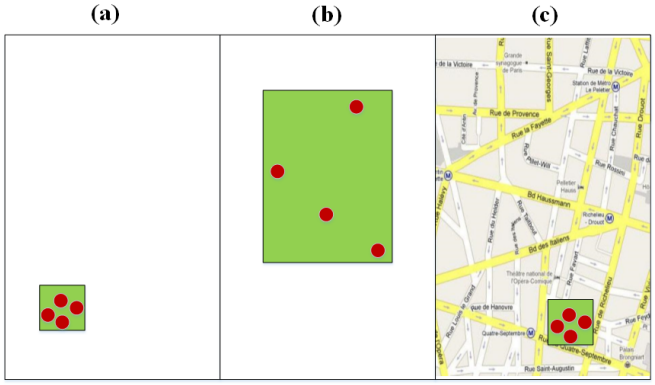


FIGURE 3.5 – Attaque d'homogénéité de localisation [2].

3.10.2.2 Attaque de position multiple (*Continuous location attack*)

1. ***Query tracking attack :*** Un adversaire pourrait lier des instantanés temporels consécutifs pour identifier l'émetteur de la requête, bien que l'information de localisation d'une requête soit camouflée en tant que régions [1]. Par exemple, considérons une requête type « trouver la station-service la plus proche dans les cinq prochaines minutes ». La durée de vie de la requête est de 5 minutes. Les attaques de suivi de requêtes deviennent possibles si un utilisateur est camouflé avec différents utilisateurs à différents moments au cours de la durée de la requête.

   Scénario d'attaque : La figure 3.4 (b) représente un exemple *d'attaque de tracking des requêtes* où il y a 11 utilisateurs mobiles et k = 5. Supposons à l'instant t_i, l'utilisateur A émet une requête continue et k = 5 anonymes. Par conséquent, les algorithmes de Cloaking donneraient une région qui contient les utilisateurs A, B, C, D, et E. En supposant aussi une distribution uniforme, un adversaire ne peut que deviner que cette requête provient de l'un de ces cinq utilisateurs dans la zone de requête. À la fois t_{i+1}, les utilisateurs mobiles changent de localisation alors que les cinq requêtes continues anonymes sont toujours en cours d'exécution. Un adversaire peut voir que la zone de requête continue contient actuellement les utilisateurs A, B, F, G et H. L'adversaire peut deviner que l'émetteur de la requête est soit A soit B en liant les instantanés de la requête continue au temps ti et t_{i+1}, car ils sont les seuls utilisateurs communs entre ces deux instantanés. De même, à l'instant t_{i+2}, l'utilisateur A est le seul utilisateur commun de la zone de requête pour les trois instantanés consécutifs, alors l'adversaire peut conclure que A est l'émetteur de la requête de l'utilisateur. L'idée est d'exploiter ***la propriété de mémorisation*** pour se défendre contre les attaques de suivi de requête. Dans la ***propriété de mémorisation***, le même ensemble d'utilisateurs devrait toujours être camouflé ensemble pendant la durée de la requête [1].

2. ***Attaques de trajectoire :*** lorsqu'une trajectoire est publiée, le propriétaire peut

être inféré par des attaquants, même si l'identificateur a été supprimé. Ces types d'attaques sont appelés attaques de trajectoire. Le problème de l'anonymisation de la trajectoire est de publier des trajectoires de telle sorte que l'anonymat de chaque trajectoire soit préservé, tandis que l'utilité des données publiées est maximisée.

3. ***Correspondance d'identité :*** l'attaquant associe plusieurs pseudonymes en fonction d'attributs égaux ou corrélés à la même identité, de sorte que la confidentialité fournie des pseudonymes modifiés est violée. Autrement dit, cette attaque peut être utilisée pour attaquer plusieurs pseudonymes d'un utilisateur [105].
4. ***Attaque de suivi de localisation (location tracking attack) :*** cette attaque utilise de nombreuses mises à jour de localisations connues de l'attaquant. Cette attaque peut être utilisée contre le changement aléatoire de pseudonymes sans utiliser de zones de mixage. Ici, même si un mécanisme d'obscurcissement est utilisé, l'attaquant peut corréler les pseudonymes successifs en reliant les informations spatiales et temporelles de requêtes ou de mises à jour de positions successives. Par exemple, un attaquant pourrait essayer de reconstruire le mouvement (trafic) des utilisateurs en fonction des emplacements disponibles de plusieurs pseudonymes [64].

   Par conséquent, à partir d'intersections, l'attaquant peut déduire où l'utilisateur se trouve, ou où sont les régions sensibles à la vie privée de l'utilisateur. Par exemple, considérons le mécanisme d'obscurcissement aléatoire qui crée différentes zones d'obscurcissement chaque fois que l'utilisateur atteint son domicile. Après cela, l'intersection de différentes zones d'obscurcissement peut être utilisée pour réduire la vie privée des utilisateurs.
5. ***Attaque du mouvement maximale :*** dans une attaque limitée de mouvement maximale [2], l'attaquant calcule la zone limitée de mouvement maximale, où l'utilisateur aurait pu se déplacer entre deux mises à jour de position ou requêtes suivantes. Comme le montre la Figure 3.6, la position de la première mise à jour effectuée au temps T1 aide l'attaquant à augmenter la précision de la mise à jour envoyée au T2. Dans cet exemple, seule une petite partie de la surface de T2 est accessible à l'intérieur de la limite de mouvement maximale. Par conséquent, l'attaquant peut exclure la partie restante de la mise à jour de position.

Il est clair que les attaques de suivi de requête sont différentes des attaques du mouvement maximal [10]. En plus, les utilisateurs peuvent encore souffrir d'attaques du mouvement maximal, même s'ils sont empêchés d'attaques de suivi des requêtes en appliquant la propriété de mémorisation à chaque requête continue. Supposons que deux requêtes continues différentes soient émises par un utilisateur mobile à un certain intervalle de temps. L'attaque du mouvement maximal représentée sur la figure 3.6 peut toujours se produire, si l'utilisateur est masqué avec différents ensembles d'utilisateurs

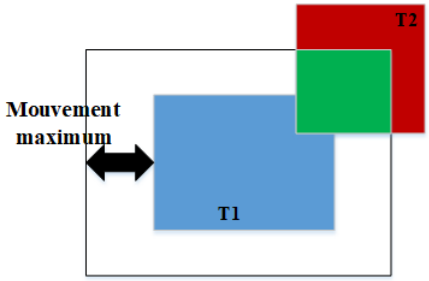


FIGURE 3.6 – Attaque du mouvement maximale [2].

pour ces deux requêtes continues. D'autre part, si l'utilisateur est toujours camouflé par le même ensemble d'utilisateurs, la région camouflée s'étendra à toute la région de service lorsque les utilisateurs se séparent et émettent de plus en plus de requêtes au fil du temps.

3.10.2.3 Attaque de liaison de contexte

Dans cette l'attaque, les informations contextuelles sont utilisées en plus des informations spatiales et temporelles. Afin de réduire la vie privée de l'utilisateur, l'attaquant peut utiliser la connaissance du contexte personnel d'un utilisateur ainsi que des connaissances antérieur tel qu'un carnet d'adresses et une carte du réseau routier, etc [114].

Pour l'attaque de liaison de contexte, nous distinguons trois types d'attaques : l'attaque de liaison du contexte personnel, l'attaque de distribution de probabilité et attaque par correspondance de la carte [2].

1. ***Attaque de liaison du contexte personnel :*** cette attaque repose sur une connaissance personnelle du contexte des utilisateurs individuels, comme les préférences ou les intérêts des utilisateurs. Par exemple, supposons qu'un utilisateur soit connu pour visiter un endroit sensible régulièrement à une certaine heure et qu'il utilise un mécanisme simple d'obscurcissement pour protéger la vie privée de son l'emplacement. Après cela, un attaquant peut augmenter sa précision d'une position obscurcie obtenue en réduisant la zone d'obscurcissement à l'emplacement des endroits sensibles dans la zone d'obscurcissement [64].
2. ***Attaque d'observation :*** ici, l'attaquant a des connaissances de l'utilisateur recueillies par l'observation. Par conséquent, l'attaque par observation est un type particulier d'attaque de liaison de contexte personnel. Par exemple, si l'attaquant pourrait voir l'utilisateur observé et que l'utilisateur utilise des pseudonymes, alors, l'attaquant pourrait retracer tous les emplacements antérieurs de l'utilisateur pour le même pseudonyme par une seule corrélation [64].
3. ***Attaque de distribution de probabilité :*** cette attaque est basée sur des informations sur le contexte environnemental et des statistiques de trafic recueillies.

L'attaquant tente ici de dériver une fonction de distribution de probabilité de la position de l'utilisateur sur la zone d'obscurcissement. Les attaquants peuvent identifier les zones où l'utilisateur se trouve avec une forte probabilité, si la probabilité n'est pas uniformément distribuée [88].

4. ***Correspondance de carte :*** ici, l'attaquant peut utiliser la correspondance de carte afin de limiter la zone d'obscurcissement à certains emplacements, conduisant à la localisation de l'utilisateur en supprimant toutes les zones inappropriées. Par exemple, la suppression des lacs de la zone d'obscurcissement réduit efficacement la taille de la zone d'obscurcissement en dessous de la taille prévue (voir la figure 3.7) [52].

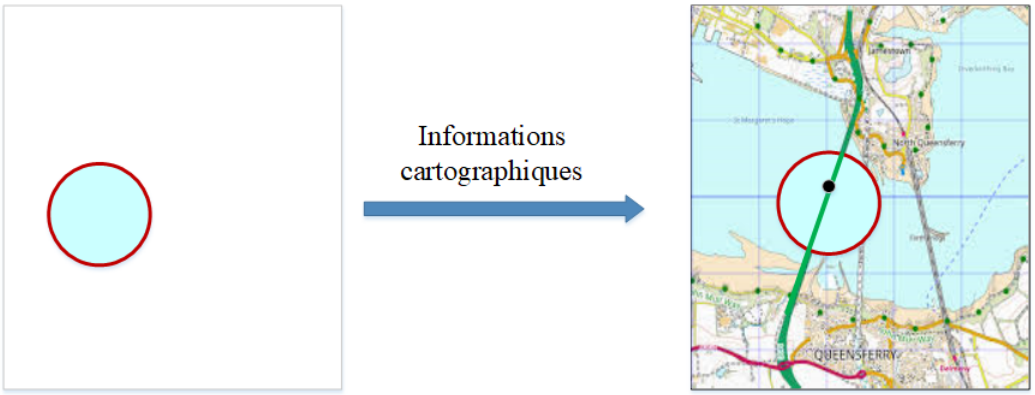


FIGURE 3.7 – Attaque de correspondance de la carte (affiner une position sur un pont routier) [2].

En plus, la carte peut fournir des informations sémantiques aux attaquants, telles que des points d'intérêt ou des types de bâtiments (hôpitaux, bâtiments résidentiels, etc). Par conséquent, l'attaquant pourrait utiliser ces informations pour restreindre davantage la taille de la zone d'obscurcissement efficace [2].

3.10.2.4 Compromis un tiers de confiance TTP

Cette attaque indique qu'un attaquant pourrait avoir accès aux données stockées sur le serveur TTP. Par exemple, un attaquant pourrait compromettre un serveur de confiance (AS) et accéder aux données utilisateur stockées. Cette attaque n'est pas prise en compte dans les approches qui reposent sur un TTP, car elle minerait chaque approche utilisant un TTP. Cependant, l'attaque d'un TTP est réaliste et non négligeable. Par conséquent, il est au moins discutable de supposer la fiabilité d'un TTP [2].

3.11 Conclusion

Les attaques de la vie privée présentent un danger primordial car elles menacent la vie privée des clients de m-business. Il est très important de mettre en oeuvre des protocoles et des mécanismes de sécurité afin de contrôler les entités du m-business, de préserver la sécurité des clients et de permettre aussi aux usagers d'utiliser le système de m-business en étant confiant.

Le prochain chapitre, nous présentons quelques travaux de recherche qui se sont intéressés à la protection de la vie privée de client dans le m-business.

Chapitre 4

Travaux connexes et synthèse bibliographique

4.1 Introduction

Dans le contexte de business mobile, il est nécessaire de protéger la vie privée des clients contre un fournisseur malveillant. Sachant que, le fournisseur malveillant (non fiable) est celui qui a l'intention de voler l'information sur les clients. En plus, Il est aussi responsable de fournir des résultats aux clients comme des réponses à la requête. Pour cela, la vie privée et la sécurité des données sont les plus grandes préoccupations dans le m-business fournissant des services LBS [115], [116].

Les problèmes de vie privée dans les applications m-business, impliquent principalement l'information personnelle de l'utilisateur mobile, les informations de localisation, les informations sur les relations sociales, les informations sur les transactions, les informations de paiement mobile, et d'autres informations liées à la vie privée [10]. Le facteur le plus important qui affecte l'adoption du m-business est la préoccupation de la divulgation des informations de vie privée liées à la localisation.

Dans la littérature, il existe plusieurs approches de protection de la vie privée, nous distinguons deux types de modèles utilisés dans ces approches. Il y a des approches basées sur les modèles de transformation géographique et d'autres approches utilisent les modèles de collaboration. Dans notre travail, nous nous intéressons aux approches basées sur les modèles de transformation géographique.

Dans ce chapitre nous présentons plusieurs travaux existants qui traitent les problèmes de protection de la vie privée de client.

4.2 Travaux existants

D'après notre étude nous avons classé les travaux existant en deux catégories : les approches à deux niveaux (deux tiers) et les approches à trois niveaux (trois tiers).

4.2.1 Approches deux tiers

Les méthodes de cette catégorie ne font intervenir que deux parties au moment de la demande : l'utilisateur et le fournisseur de services. En plus, la plupart de ces méthodes supposent qu'aucune connaissance antérieure n'est disponible pour l'attaquant. Comme par exemple, le travail de PROBE [97] suppose que l'attaquant connaît tous les endroits sensibles. Une solution simple pour la vie privée des requêtes est de générer un certain nombre de requêtes redondantes pour chaque requête réelle. Par exemple, le client mobile CM pourrait générer des «faux» emplacements aléatoires et envoyer des requêtes redondantes au système m-business, en plus de la requête contenant l'emplacement réel de client mobile CM. Une telle approche est adoptée dans [81], où des emplacements factices sont générés de telle sorte que les trajectoires résultantes imitent des modèles de mouvement réalistes. Les algorithmes de génération des Dummies (localisations factices) peuvent tenir compte des paramètres de mouvement, comme la vitesse, et de certaines contraintes, comme un réseau routier (Road Network).

Dans cette section nous présentons les travaux connexes de catégorie deux tiers : Dans [117], Yiu et al présentent leur infrastructure appelée SpaceTwist pour répondre aux k plus proches voisins des requêtes (k-nearest-neighbor-queries K-NN) tout en protégeant la vie privée de la localisation des utilisateurs. Dans l'approche de SpaceTwist, au lieu de générer plusieurs emplacements, il utilise un protocole de requête incrémentielle pour le voisin le plus proche, basé sur un emplacement d'ancrage.

Les utilisateurs envoient une soi-disant "Ancre" représentant un emplacement incorrect (fictif), au lieu d'envoyer des localisations précises de l'utilisateur à fournisseur de services. L'ancre est initialement définie sur un emplacement généré aléatoirement par l'utilisateur. L'ancre est ensuite utilisée pour demander itérativement points de données pour des différentes distances par rapport à l'ancre. L'utilisateur calcule ensuite les résultats de la requête en fonction de sa position exacte et des points de données reçus.

Par conséquent, dans [117], les résultats de requête précis sont présentés à l'utilisateur. Cependant, la vie privée de la localisation est obtenue grâce à des coûts de requête et de communication plus élevés.

Une autre approche avancée d'obscurcissement a été fournie par Damiani et al [97]. Dans ce travail, les auteurs proposent un système PROBE pour protéger la vie privée des emplacements sémantiques, en empêchant l'association entre utilisateurs et emplacements critiques tels que les hôpitaux. Leur approche de l'obscurcissement cartographique étend la zone d'obscurcissement de manière adaptative, de sorte que la probabilité pour l'utilisateur de se trouver dans un certain lieu sémantique est inférieure à un seuil donné.

Dans PROBE, il est supposé que l'attaquant a accès à tous les emplacements sensibles à partir d'un espace de données particulier (par exemple, une ville, un pays, etc.).

En plus, les emplacements sensibles sont représentés par des entités, classées en types d'entités (hôpitaux, restaurants, etc.). Dans une phase hors ligne, une carte masquée est construite en divisant l'espace en un ensemble de régions disjointes de sorte que la probabilité d'associer chaque région à un certain type d'entité est limitée par un seuil. La figure 4.1 montre une carte masquée avec deux régions masquées (R_1 et R_2) : aucune région ne peut être associée au type d'entité "hôpital" avec une probabilité supérieure à 40 %. Où R_1 contient au total 80 cellules de grille, dont 32 sont sensibles et $32/80 = 0,40$ et R_2 contient au total 130 cellules de grille, dont 42 sont sensibles et $42/130 = 0,32$. Un autre aspect intéressant de PROBE (comme indiqué dans [118]) est qu'il peut être étendu pour protéger l'inférence lorsque les utilisateurs se déplacent dans différentes régions masquées.

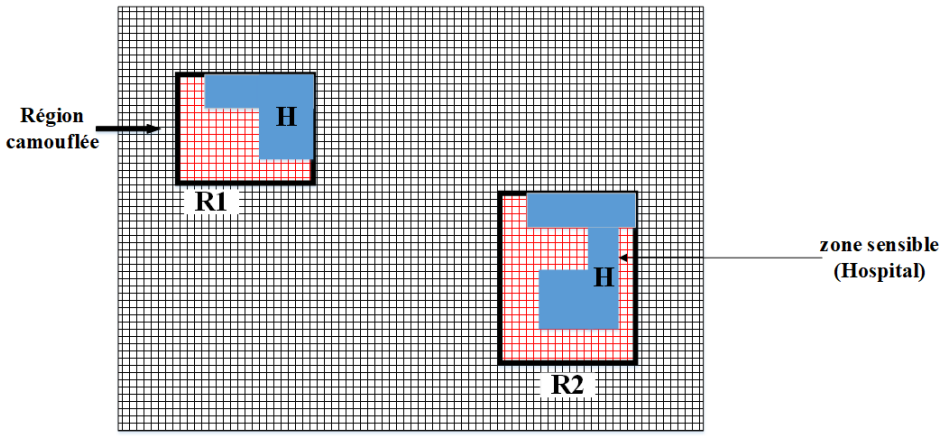


FIGURE 4.1 – la probabilité d'association au type de caractéristique « hôpital » est inférieure à 44 %.

PROBE offre une confidentialité supérieure aux autres méthodes de catégorie de $2-Tiers$. Cependant, aucune des solutions de transformation spatiale à deux niveaux ne peut empêcher la ré-identification de la source de la requête si un attaquant a des informations sur des emplacements utilisateur spécifiques. Ceci est un exemple de violation de la vie privée de l'utilisateur, si l'utilisateur u émet une requête et cet utilisateur situé dans un emplacement éloigné, par conséquent, un attaquant qui sait que l'utilisateur u est la seule personne résidant dans cette zone peut associer l'utilisateur u à la requête.

La catégorie suivante de méthodes d'anonymisation des requêtes traite ce type de problème.

4.2.2 Approches trois tiers

Dans cette section nous allons présenter les travaux connexes de catégorie tierce (TTP), nous allons aussi identifier leur utilité.

Dans [10], les auteurs proposent un algorithme de camouflage de l'emplacement (Location cloaking), appelé ICliqueCloak, pour se défendre contre les attaques dépen-

dantes de la localisation. L'idée principale de ce travail est de conserver progressivement les cliques maximales nécessaires pour le camouflage d'emplacement dans un graphe non dirigé qui tient compte de l'effet des mises à jour continues de l'emplacement.

La solution proposé dans [10], est que l'algorithme est conscient de la région de camouflage de client A en t_i (R_A, t_i) et la limite maximale du mouvement de client A en t_i (MMBA, t_i, t_{i+1}), et tente de trouver la région de camouflage pour A dans MMBA, t_i, t_{i+1}. Même si l'attaquant connaît la limite de vitesse de chaque utilisateur, il ne peut toujours pas indiquer l'emplacement exact de A dans la région R_A, t_i et dans la région R_A, t_{i+1}. Cependant, lorsque l'attaquant peut savoir que les nouveaux éléments de Cloaking au moment ti ne sont pas membres de la région de camouflage précédente de l'utilisateur mobile (demandeur) au moment t_{i-1}, cela peut entraîner de graves violations de la vie privée. C'est parce que les auteurs n'ont pas pris en compte la similarité de mouvement des utilisateurs.

En outre, dans cet article, une nouvelle demande n'est pas délivrée avant que la dernière soit desservie. C'est-à-dire, à chaque fois, un utilisateur peut être associé à une seule demande de requête.

En plus, l'algorithme de [10] ne satisfait que l'anonymat de la région de camouflage actuelle (t_i) et ne satisfait pas l'anonymat de la région de camouflage précédente (t_{i-1}). En outre, le coût de l'anonymisation de cet algorithme est légèrement augmenté par rapport aux autres algorithmes.

De toute évidence, le fait d'abandonner la requête de l'utilisateur évaluera le système comme étant peu fiable. Comme dans cet algorithme, le client avec un niveau élevé de vie privée est abandonné dans le cas de transformation de l'ensemble de candidat négative à positif. Dans l'algorithme de [10], il existe d'autre cas de rejet les requêtes de l'utilisateur, si la nouvelle limite de la région étendue n'est pas encore couverte par le MMB précédent de chaque utilisateur.

Le travail proposé dans [119] se concentre sur deux méthodologies pour assurer la vie privée de touristes par l'anonymisation du contexte de localisation. Le processus d'anonymisation s'effectue grâce à la création des régions de camouflage basées sur la clique dans les contextes statiques et dynamiques. Cependant, les auteurs de [119] ne proposaient rien de nouveau par rapport aux travaux de [95], [9]. En plus, dans le travail de [119], il existe des cas de rejet les requêtes de touristes.

En outre, les auteurs de [119] n'ont pas pris en compte la similarité de mouvements des touristes. Cela peut entraîner de graves violations de la vie privée lorsque les touristes qui sont cachés dans la même région, ils ont des directions ou une vitesse différentes.

Jungho Um et al [120] proposent un algorithme de camouflage pour la protection de la vie privée dans LBS. Cet algorithme peut prendre en charge à la fois K-anonymat et L-diversité. En d'autres termes, cet algorithme crée une région de camouflage minimale en trouvant L bâtiments (l-diversité), qui contient au moins un utilisateur. Il calcule

ensuite le nombre d'utilisateurs existant dans la région de camouflage. Si le nombre d'utilisateurs ne satisfait pas k-anonymat, il étend la cellule jusqu'à ce qu'elle satisfasse du k-anonymat. Pour générer la région de camouflage minimal, les auteurs utilisent une structure de grille pour stocker les bâtiments et les utilisateurs ainsi qu'une technique d'élagage (pruning) pour réduire les calculs inutiles. Dans ce travail [120], les auteurs traitent les problèmes de Privacy Grid [14].

Dans Privacy Grid [14], les auteurs proposent une architecture permettant de prendre en charge les requêtes anonymes basées sur la localisation dans les systèmes d'envoi d'informations mobiles. Mais, Privacy Grid n'est pas satisfaisante pour soutenir l-diversité de manière appropriée. C'est parce que le même bâtiment peut être compté autant de fois que le nombre de cellules de grille où le bâtiment est situé. En outre, Privacy Grid ne se préoccupe pas si les bâtiments contiennent un utilisateur ou non. Par conséquent, les auteurs de [120] proposent une solution à ce problème, en proposant un algorithme de camouflage qui compte la construction juste une seule fois et assure que la construction comprend au moins un utilisateur.

Dans [121], les auteurs proposent une architecture permettant de création des régions de camouflage basé sur la grille afin de soutenir les requêtes continues dans LBS. En particulier, les auteurs proposent une méthode de génération des régions de camouflage qui réduit la probabilité d'exposition d'un utilisateur mobile à un niveau minimum ; cette méthode calcule un degré de protection de la vie privée en accordant des poids aux utilisateurs mobiles. En outre, par l'utilisation de l'arbre des informations de recherche basée sur la largeur (an information Tree), les auteurs de [121] traitent le problème des frais généraux de calcul. Avec cet arbre, ils peuvent explorer rapidement toutes les régions de camouflage possibles et l'algorithme trouve la région de camouflage temporaire de taille minimale. Cependant, la méthode proposée dans ce travail est très compliqué, les auteurs utilisent des échantillons des données (20 régions précédentes) pour calculer la matrice de transition.

Dans [122], les auteurs introduisent un algorithme pour la protection de la vie privée des requêtes continues de LBS qui considère la similarité des utilisateurs (la vitesse et la direction) pour l'anonymisation. Cependant, les auteurs se concentrent uniquement sur la vie privée des requêtes, ils n'abordent pas la vie privée de l'emplacement.

Même dans l'article de [11], les auteurs se concentrent sur la vie privée des requêtes. Dans ce travail, les auteurs présentent un algorithme de préservation de la vie privée des requêtes continues (V-DCA) pour LBS en tenant compte de la similarité de la vitesse et de l'accélération de l'utilisateur. Mais, ce travail est faible contre l'attaque de localisation. Les auteurs de [11] suggèrent une idée pour réduire la complexité de l'algorithme tout en respectant les exigences de vie privée, qui est l'utilisation des ensembles de camouflage qui sont créés respectivement pour créer la nouvelle région de camouflage. Cependant, l'algorithme de **V-DCA** [11] présente la complexité dans le cas de la recherche et découvrir des utilisateurs les plus proches.

De plus, dans cet algorithme, il existe des cas de rejet les requêtes des utilisateurs, dans le cas où les utilisateurs n'ont pas la même vitesse ou la même accélération, cet algorithme supprime les requêtes des utilisateurs. En plus, dans le cas où le **MBR** des utilisateurs est inférieur au seuil δ_q ou le nombre des utilisateurs de l'ensemble de camouflage est inférieur à k_{global}, les requêtes sont rejetées.

Il existe des autres travaux qui utilisent les mannequins (Dummies) comme concept pour augmenter la vie privée des systèmes. Kido et al [81] introduisent le concept de génération des localisations factices (fictives) mais ils ont seulement considéré l'architecture du serveur client. Dans le travail de [81], le client envoie la position réelle avec les positions fictives au fournisseur de services. Ensuite, le fournisseur répond avec des réponses à la fois à la position vraie et à la position fictive. Cependant, les coûts de traitement sur l'appareil mobile sont élevés pour filtrer les résultats. En outre, il existe un coût de communication très élevé entre le client et le fournisseur de services. Un autre inconvénient, dans [81] le client peut être ré-identifié si un adversaire a une connaissance historique et en prenant l'intersection de toutes les régions avec lesquelles un adversaire est sûr que le client unique a envoyé une requête.

En outre, le travail dans [123] se concentre sur les systèmes basés sur le client-serveur où le serveur d'anonymisation n'est pas présent. Encore, ils se concentrent aussi sur les trajectoires fictives pour éviter l'identification de trajectoires réelles.

Il y a pas mal d'approches qui utilisent le concept k-anonymat pour assurer la vie privée de la localisation. Mokbel et al proposent une structure de Casper dans [15]. Les auteurs calculent la région de Cloaking des k utilisateurs basés sur des valeurs de k défini par l'utilisateur et sur des valeurs de zone A_{min} indiquant que l'utilisateur veut cacher son emplacement dans une taille de surface d'au moins A_{min}. Casper est basé sur les Quadtrees. Un Quadtree divise récursivement l'espace en quadrants jusqu'à ce que les points de chaque quadrant correspondent à un nœud [124].

Une idée similaire a été présentée par Ghinita et al [118] pour leur approche de camouflage spatio-temporel. Pour améliorer la vie privée fournie par le camouflage spatial, les auteurs prennent en compte la connaissance antérieure (background) de la carte représentée par un ensemble de caractéristiques sensibles à la vie privée. De plus, cette méthode résiste aux attaques basées sur la vitesse maximale connue des objets, voir l'attaque de MMB (maximum movement boundary).

Dans [9] et [125] Gedik et al proposent une approche qui effectue un camouflage spatial et temporel pour calculer l'ensemble de k-anonymat. Afin de préserver une qualité de service acceptable, dans cette approche l'utilisateur peut définir des limites supérieures individuelles pour la taille de la zone camouflage et les périodes associées aux les localisations. L'approche utilise le camouflage temporel en retardant les mises à jour afin que le nombre souhaité de k utilisateurs soit déterminé dans l'intervalle de temps et la zone de camouflage maximum qui sont déterminés par l'utilisateur.

Le concept de base de k-anonymat a été étendu grâce à diverses approches visant

à renforcer la protection de la vie privée. Les extensions les plus importantes sont : strong k-anonymity, l-diversity et historical k-anonymity.

Zhang et al [126] garantissent un strong k-anonymat en s'assurant que le groupe (cluster) calculé de k utilisateurs reste le même sur plusieurs requêtes (la réciprocité des k-clusters). Par conséquent, les attaques qui croisent plusieurs k-clusters de requêtes différentes ne peuvent pas d'identifier facilement un utilisateur.

Bamba et al [14] présentent l'idée de l-diversité de la localisation, est que l'emplacement de l'utilisateur ne peut pas être déterminée à partir d'un ensemble de l différents emplacements physiques tels que des cliniques. À cette fin, l'approche garantit que la localisation des membres du cluster est non seulement différente, mais aussi assez éloignée les uns des autres. Dans le cas contraire, si toutes les positions de l'utilisateur appartiennent au même emplacement sémantique, un attaquant connaîtrait l'emplacement de l'utilisateur cible avec une faible imprécision.

Habituellement, les approches de cloaking basées k-anonymat nécessitent un tiers qui agit comme un anonymiseur (TTP) qui est au courant de toutes les localisations des utilisateurs. Ainsi, il existe plusieurs approches qui tentent d'éviter un anonymiseur de confiance, c'est-à-dire d'appliquer une approche décentralisée telle que [7] et [72].

Par conséquent, pour trouver une région spatiale qui couvre le nombre nécessaire d'utilisateurs du cluster (k), Chow et al [7] utilisent la communication peer-to-peer (P2P). Une fois que le cluster requis est trouvé, un membre du cluster sélectionné de manière aléatoire envoie la requête prévue au fournisseur afin de masquer l'identité de l'expéditeur de la requête. Ghinita et al [72] proposent une approche P2P appelée MobiHide afin de cacher l'initiateur de requête parmi un groupe de k utilisateurs par l'utilisation des courbes de remplissage d'espace Hilbert.

4.3 Compariasons entre les travaux existants

Le tableau 4.1 présente des comparaisons entre quelques travaux existants dans la littérature.

TABLE 4.1 – Tableau de comparaison des travaux connexes.

	Goals of Privacy			**Attacker knowledge**					**Static Dynamic**	**Privacy Protection Types**		**Privacy Metrics**
	Localisation	***ID***	***Time***	***Location Attack***	***Linking Attack***	***Query Tracking***	***Query Sampling***	***Homogeneity Attack***	***Snapshot / Continuous***	***Query Privacy***	***Location Privacy***	
[10] 2012	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	C	Non	Oui	2
[122] 2015	Non	Oui	Oui	Non	Oui	Oui	Non	Oui	C	Oui	Non	2
[119] 2016	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	S/C	Non	Oui	2
[120] 2009	Non	Non	Oui	Non	Non	Non	Non	Non	S	Non	Oui	2
[14] 2008	Non	Non	Oui	Non	Non	Non	Non	Non	S	Non	Oui	2
[121] 2012	Non	Non	Oui	Non	Non	Non	Non	Non	C	Oui	Non	1
[11] 2012	Non	Oui	Oui	Non	Oui	Oui	Oui	Non	C	Oui	Non	1
Notre Approche	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	S/C	Oui	Oui	3

4.4 Métriques existantes de protection de la vie privée

La métrique de la vie privée représente l'outil utilisé pour valider le respect d'un mécanisme de protection de la vie privée à un ensemble des exigences de vie privée. En plus, une métrique de confidentialité décrit l'ensemble des critères formels qui servent à quantifier le niveau de protection assurée par un mécanisme donné, et cela par rapport à des objectifs de protection prédéfinis [61]. Le choix et la conception d'une métrique dépendent principalement du paradigme utilisé dans un mécanisme, ainsi que les objectifs qu'il doit atteindre.

Les mesures de protection de la vie privée servent de base à l'évaluation et à la comparaison des modèles de protection de la vie privée ainsi qu'à l'adaptation de ces modèles aux exigences des utilisateurs en matière de protection de la vie privée. Intuitivement, une métrique de la vie privée mesure la difficulté pour l'adversaire de deviner les données réelles à partir des données transformées [88]. Cela signifie que le niveau de vie privée dépend de ce qu'un adversaire sait. Les capacités de l'adversaire sont spécifiées dans le modèle de l'adversaire qui décrit : a) la connaissance auxiliaire de l'adversaire (connaissance antérieur) ; b) les capacités d'inférence [88].

En particulier, les auteurs de [61] introduisent trois critères de classification qu'ils appellent : sujet, usage et paradigme, expliqués dans ce qui suit :

- ✓ ***Sujet :*** Le sujet précise si la mesure se réfère à l'utilisateur unique ou, inversement, à un groupe d'utilisateurs. Le sujet précise ainsi la granularité sociale de la mesure de la vie privée. Pour distinguer les deux cas, nous disons que la métrique est individuelle et collective, respectivement.
- ✓ ***Usage :*** L'utilisation spécifie à quelle étape de l'application la métrique est utilisée et dans quel but. Les auteurs de [61] considèrent les deux cas suivants :
  - La métrique est utilisée à la fin d'une période d'observation pour évaluer le niveau de protection de la vie privée fourni au Sujet par le mécanisme de protection de la vie privée dans un tel délai. Nous disons que la métrique est **ex-post**.
  - La métrique est utilisée avant l'application du mécanisme de protection des renseignements personnels afin d'adapter la transformation au degré de protection requis. Nous disons que la métrique est **ex-ante**.
- ✓ ***Paradigme :*** Les mesures de la protection de la vie privée reposent généralement sur des paradigmes comme : k-anonymat, les mesures fondées sur l'entropie, les mesures fondées sur les erreurs, les mesures fondées sur des modèles probabilistes et la protection de la vie privée différentielle.

4.4.1 Métriques computationnelles

Les métriques de cette catégorie utilisent des méthodes et des règles de calcul bien définies afin d'évaluer la vie privée assurée par un mécanisme de protection. Elles sont le plus souvent utilisées dans des mécanismes basés sur l'obscurcissement, et ne prennent pas en considération l'adversaire ou l'utilité souhaitée [80].

4.4.1.1 K-anonymat de l'emplacement (Location k-anonymity)

Une métrique computationnelle parmi les plus connues dans ce contexte est l'adaptation de k-anonymat aux services m-business [45]. K-anonymat de localisation mesure le degré d'anonymat de l'utilisateur lorsque le flux d'informations est sporadique, par exemple [127], [64]. L'adversaire peut ré-identifier les utilisateurs apparemment anonymes en reliant leur emplacement à une source externe se référant au même emplacement et en révélant l'identité de l'utilisateur [61].

Le concept de k-anonymat a été initialement proposé pour la publication confidentielle des données (Private Data Publishing), et a été rapidement adopté dans plusieurs domaines, incluant les services m-business. Le niveau de vie privée est mesuré en fonction de la valeur k, qui indique si un adversaire peut ré-identifier un utilisateur dans un groupe de k utilisateurs. Ainsi, nous disons qu'un mécanisme est k-anonyme s'il peut assurer que l'utilisateur n'est pas identifiable parmi au moins k-1 autres utilisateurs.

K-anonymat de l'emplacement est naturellement associé à un mécanisme de dissimulation de l'emplacement (l'obscurcissement). Par conséquent, la vie privée dans les mécanismes de protection des emplacements est exprimée par des zones géographiques. De ce fait, l'adaptation de k-anonymat est liée aux mécanismes qui se basent sur l'obscurcissement, et remplacant les coordonnées géographiques d'un utilisateur par une région plus large dont le but est de le protéger. Ainsi, on dit qu'une région obscurcie R est $k - anonyme$ si R est indiscernable parmi $k - 1$ autres régions à proximité.

Plus formellement, une région obscurcie est k-anonyme si la probabilité de réidentification de la position d'un utilisateur est égale à 1/k. L'utilisation d'une métrique basée sur k-anonymat se fait souvent avant la génération de la région protégée, la métrique est donc utilisée ex-ante. La valeur de k est utilisée pour générer la région obscurcie [61], comme le montre la figure 4.2. De plus, la valeur de k peut être soit unique pour l'ensemble des utilisateurs, soit personnalisée comme dans [9]. Par conséquent, la métrique peut être collective ou individuelle.

La condition d'emplacement indiscernable, cependant, ne sert qu'à protéger l'association entre les utilisateurs et les requêtes, tout en n'empêchant pas la divulgation de l'association entre les utilisateurs et les emplacements [61]. Par exemple, si tous les k utilisateurs se trouvent dans une petite région, par exemple, un hôpital, l'emplacement est facilement révélé. Par conséquent, malgré sa popularité, K-anonymat de l'emplacement ne garantit pas une réelle protection de l'emplacement [128], [129]. Pour cela,

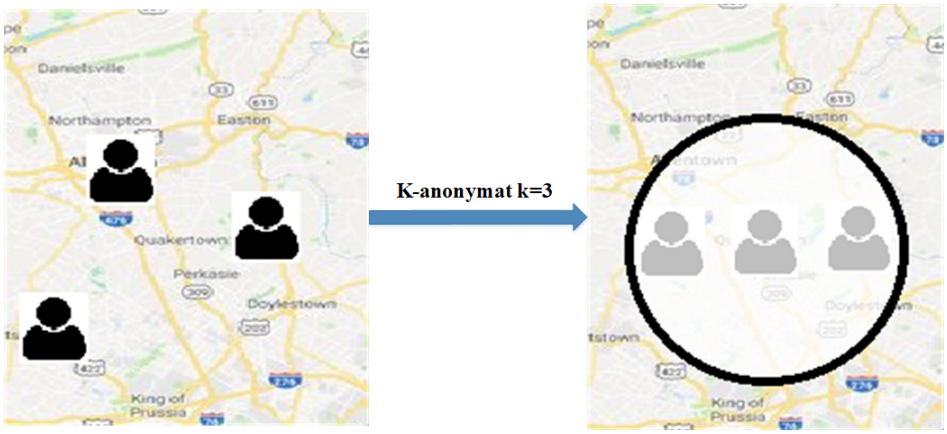


FIGURE 4.2 – Exemple de k-anonymity (k = 3).

une autre métrique (l-diversité de localisation) a été définie.

4.4.1.2 L-diversité

L-diversité complète k-anonymat pour empêcher l'identification des emplacements sémantiques, c.-à-d. des endroits, dans lesquels l'utilisateur peut être situé dans une région obscurcie. Une première définition de l-diversité de localisation est donnée dans [14] : La région est hétérogène lorsqu'elle contient des emplacements physiques différents où un emplacement physique est identifié par une adresse symbolique. Une définition différente, qui tient compte de la sémantique de l'emplacement ; une région R est l-diversité si les emplacements sémantiques contenus dans R sont d'au moins l types différents [130].

4.4.2 Métriques probabilistes

Les métriques probabilistes décrivent l'adversaire en termes probabilistes. L'adversaire utilise les connaissances antérieures en les corrélant avec les coordonnées géographiques récupérées, pour déduire l'emplacement réel de l'utilisateur. Les connaissances antérieures sont souvent exprimées par des variables aléatoires, et les capacités d'inférence par des modèles statistiques d'inférence.

4.4.2.1 Métriques basées sur les entropies

L'entropie est une mesure du degré moyen d'incertitude associé à un ensemble d'événements. Plus formellement, l'entropie associée à un ensemble contenant N éléments est définie par :

$$h = -\sum_{i=1ton} p_i log p_i \tag{4.1}$$

Où, p_i représente la probabilité d'occurrence de l'événement i. Dans le contexte de

m-business, les entropies ont été utilisées comme base à plusieurs métriques d'évaluation de la vie privée (comme Mix-zones, Feeling-based location privacy). En résumé l'adaptation des entropies implique le calcul d'incertitude liée à l'application d'un mécanisme donné [61].

4.4.2.2 Mix-zones

le mécanisme Mix-Zones [105] protège les utilisateurs par l'interdiction des requêtes dans une zone prédéfinie, et la confusion des pseudonymes des utilisateurs au moment de la quitter. En d'autres termes, les auteurs du mécanisme Mix Zones utilisent des zones géographiques prédéfinies dans lesquelles aucune information sur l'emplacement n'est divulguée (c.-à-d. que l'emplacement est supprimé). À l'intérieur de la zone de mixage, un nouveau pseudonyme est attribué à l'utilisateur jusqu'à la prochaine zone de mixage est entré.

L'objectif est d'empêcher le suivi du mouvement à long terme de l'utilisateur, c.-à-d. si un pseudonyme est violé, seul le mouvement correspondant à la trace associée à ce pseudonyme serait révélé [61]. Un exemple de Mix Zones est donné à la Figure 4.3.

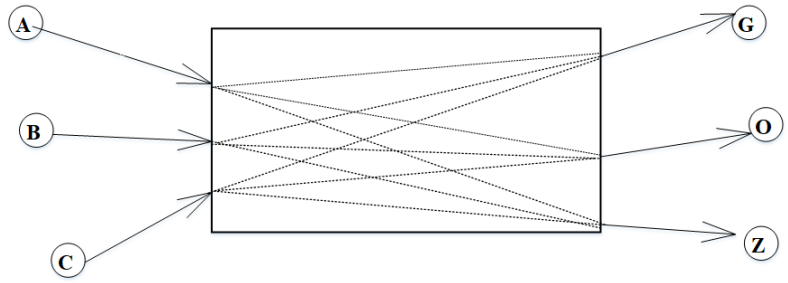


FIGURE 4.3 – Mix Zones.

L'évaluation de ce mécanisme se fait par la mesure de l'incertitude de la corrélation entre les pseudonymes anciens et nouvellement générés [61]. De façon plus formelle, considérons un ensemble d'utilisateurs N qui entrent dans une zone d'interdiction (mix zone) X avec la liste des pseudonymes P = $p_1, p_2, ..p_n$ ou chaque pseudonyme est associé à un utilisateur. Le même groupe d'utilisateurs N quittera la zone X après le temps δ_t avec d'autres pseudonymes représentés par l'ensemble Q = $q_1, q_2, ..q_n$. Le rôle des entropies dans un tel mécanisme est de mesurer l'incertitude de l'association entre les éléments de P et Q sur δ_t, et qui est formulée avec la probabilité de trouver un ensemble M = $m_1, \ldots, m_k$ qui contient toutes les similarités (un ensemble mappages possibles) entre P et Q :

$$h = -\sum_i Pr(m_i|M) log Pr(m_i|M) \tag{4.2}$$

Notez que la mesure d'entropie dépend du nombre d'utilisateurs entrant dans Mix-Zones et que ce nombre n'est connu qu'au moment de l'exécution. Par conséquent, la

métrique de confidentialité, définie dans ces termes, ne peut être utilisée qu'ex-post, en tant que métrique collective.

À ce jour, la plupart des techniques existantes dans la littérature sur la protection de la vie privée adoptent largement deux mesures de vie privée populaires (telles que le k-anonymat et entropie) mais sont principalement centralisés (c.-à-d. sont basés sur serveur de localisation de confiance).

4.5 Conclusion

Les différentes approches de protection de la vie privée de l'emplacement sont nécessaires pour atteindre les différents objectifs de protection. Comme nous l'avons vu, aucune approche n'est adaptée pour protéger tous les objectifs de protection énoncés en même temps.

Dans ce chapitre, nous avons étudié et élaborer une synthèse d'un ensemble de travaux qui traitent le problème de protection de la vie privée de client. L'étude comparative de ces travaux est la base de notre contribution qui sera présentée dans le prochain chapitre.

Chapitre 5

Contribution : Une approche de sécurité pour le m-business

5.1 Introduction

De nos jours, la protection de la vie privée représente l'un des problèmes majeurs dans le m-business. Parce que les clients veulent protéger leurs informations personnelles lors de la demande du service (comme l'identité et l'emplacement). En outre, la divulgation de l'emplacement exact des clients soulève de graves préoccupations en matière de protection de la vie privée, car les emplacements peuvent donner des renseignements sensibles sur l'état de santé des personnes, les affiliations politiques et religieuses, etc.

La protection de la vie privée des emplacements est une exigence essentielle pour le déploiement réussi d'applications m-business basées sur l'emplacement [83]. À l'heure actuelle, il existe plusieurs scénarios dans lesquels une certaine forme de partage d'emplacement est nécessaire et pour lesquels la vie privée doit être préservée. Premièrement, les utilisateurs envoient des requêtes basées sur la localisation à des serveurs non fiables qui stockent des bases de données de points d'intérêt. Dans ce cas, l'objectif de la protection de la vie privée est de permettre aux clients de récupérer les points d'intérêt à proximité sans avoir à divulguer les emplacements exacts au fournisseur de services de localisation. Deuxièmement, les fournisseurs des services recueillent de grandes quantités de données de localisation, soit sous forme d'échantillons instantanés de localisation, soit sous forme de trajectoires, c'est-à-dire des séquences de relevés de localisations consécutives correspondant au même utilisateur. Ces ensembles de données, s'ils sont rendus publics, peuvent être utilisés à des fins de recherche ou à d'autres fins d'intérêt public. Cependant, les données doivent être épurées, pour empêcher un adversaire d'associer des instantanés de localisation ou des trajectoires avec les identités des utilisateurs.

Comme déjà mentionné dans les chapitres précédents, un aperçu de l'état de l'art

en matière de la protection de la vie privée de l'emplacement. Un ensemble diversifié de solutions est examiné, y compris des techniques d'anonymisation utilisant la généralisation de l'emplacement, les techniques cryptographiques et les transformations géométriques.

Dans ce chapitre, nous allons présenter nos contributions [131] et l'architecture générale de notre approche. Ensuite, nous allons expliquer l'architecture détaillée de chaque composant et son fonctionnement, nous allons terminer ce chapitre par une conclusion.

5.2 Motivation et idées de base

Dans le m-business, les clients veulent être en sécurité contre les adversaires ou les fournisseurs de services qui sont indignes de confiance. Il existe des travaux qui adoptent un seul mesure de vie privée (Privacy) comme [9], et d'autres adoptent deux mesures en même temps comme [10]. Pour résoudre le problème de la vie privée de l'utilisateur, k-anonymat de l'emplacement et granularité de camouflage sont deux mesures de vie privée couramment utilisées [10] :

- ✓ ***K-anonymat de l'emplacement :*** un utilisateur mobile est considéré comme un k-anonymat de l'emplacement si et seulement si les informations de localisation envoyées au fournisseur de services ne peuvent être distinguées de celles d'au moins k-1 autres utilisateurs. Pour obtenir le k-anonymat de l'emplacement, les emplacements exacts des utilisateurs sont étendus aux régions masquées de sorte que chaque région couvre au moins k utilisateurs.
- ✓ ***Granularité de camouflage :*** elle exige que la zone de la région masquée soit plus grande qu'un seuil spécifié par l'utilisateur.

Bien que le k-anonymat de l'emplacement protège l'identité de l'utilisateur (sur k utilisateurs), il peut ne pas être en mesure d'empêcher la divulgation de l'emplacement (par exemple, une région de camouflage couvrant k utilisateurs dans les zones peuplées peut être très petite). D'un autre côté, la granularité du camouflage empêche la divulgation de l'emplacement mais ne peut pas se défendre contre les attaques pour les identifiants des utilisateurs dans les cas où les emplacements des utilisateurs sont connus publiquement et où il n'y a qu'un seul utilisateur dans la région masquée.

Par conséquent, nous adoptons trois mesures de vie privée dans le même processus de protection : l'anonymat de l'emplacement (k-anonymat), la granularité de camouflage (the cloaking granularity) et la mobilité des clients, nous avons pris en considération la similarité de mouvement des clients : la similarité de vitesse et la similarité de direction. En effet, du fait que le client peut envoyer ses requêtes de n'importe où et n'importe quand, nous devons prendre en considération l'ensemble des emplacements des clients quand ils se déplacent. Cela nous motive à combiner la métrique de la

mobilité des clients avec les deux autres métriques. De cette façon, nous améliorons l'efficacité de notre processus de protection de la vie privée de client (*user privacy*).

Notre processus de protection de la vie privée des clients dans le m-business est basé sur des différents mécanismes de camouflage (Cloaking Mechanisms). Par rapport aux algorithmes de Cloaking qui sont présentés dans [9], [10]. Ils ne considèrent que la protection de la vie privée de l'emplacement. Cependant, un adversaire ne devrait pas pouvoir lier une requête à un client mobile spécifique (Query Privacy). Par conséquent, dans notre travail, nous nous occupons la protection de la vie privée des clients mobiles dans m-business en empêchant les adversaires d'être au courant de l'emplacement actuel ou passé du client mobile (ce type de protection s'appelle Location Privacy) ainsi qu'empêcher les adversaires de lier une requête ou une réponse spécifique à un client mobile spécifique (ce type de protection s'appelle Query Privacy).

En outre, les auteurs de [9], [14], [120] et [13] ont défini une solution pour la protection de la vie privée uniquement pour la requête instantanée (snapshot query). Par conséquent, ils ne traitent pas les attaques dépendantes de la localisation, tandis que notre approche est concernée par la protection de la vie privée pour les requêtes continues (*Continuous queries*).

De plus, les auteurs dans [10], n'ont pas pris en compte les mouvements de clients mobiles dans leur processus. Dans notre approche, afin de construire la région de cloaking, nous prenons en compte la similarité de mouvement pour sélectionner l'ensemble de candidats.

Il existe des facteurs qui influent sur l'emplacement du client mobile à l'avenir : les emplacements à l'heure actuelle, la vitesse du client, l'accélération du client et la direction du client. La vitesse décrit la modification de la position d'un client au cours du temps, l'accélération décrit la modification de la vitesse au cours du temps. Par conséquent, la vitesse et l'accélération affectent les emplacements des clients mobiles dans le futur (dans les instantanés suivants). Même si les clients se déplacent avec une accélération et vitesse similaires, cela ne pas signifier que les clients restent ensemble à l'avenir, parce que les clients ne se déplacent pas nécessairement dans la même direction, leur similarité dans la direction est aussi très importante pour protéger efficacement leur vie privée.

Ainsi, nous allons utiliser la similarité de vitesse, la similarité de direction et la similarité d'accélération (Définition 13) pour sélectionner l'ensemble de candidats EC (Définition 15). Puisque les clients mobiles qui ont une direction, une vitesse et une accélération similaires sont plus susceptibles de rester ensemble à l'avenir pour protéger efficacement leur vie privée. D'où, il est clair que les clients qui restent ensemble impliquent une plus petite région de camouflage et donc une meilleure *QoS*.

Notre approche s'appuie sur un tiers de confiance, appelé TTP, qui joue le rôle de médiateur entre l'utilisateur et le fournisseur de services. K-anonymat garantit que l'émetteur de la requête ne peut pas être uniquement reconnu par un regroupement

d'utilisateurs K.

Dans le m-business, la notion de k-anonymat s'interprète comme suit : s'assurer qu'une attaque tenant compte de l'emplacement de la requête ne sera pas en mesure de distinguer la source de la requête avec une probabilité supérieure à $1/K$ [132].

En plus, les approches centrales comme [13], [9], [14], [15] seront sous-performances, si les k-1 autres clients ne sont pas disponibles au moment de la requête de client mobile.

Au moment de la requête, le moteur d'anonymisation a deux options si les k-1clients ne sont pas présents :

- ✓ Attendez que k-1 d'autres requêtes soient effectuées dans la même région [9].
- ✓ Étendre la région à la recherche de k-1 autres requêtes [15], ou continuer à diviser une grande région jusqu'à ce que la région contienne plus de k-1 autres clients [14].

Si le serveur central TTP ne peut toujours pas répondre à l'exigence de k-anonymat après l'expansion de la région ou l'attente de k-1 autres clients, la requête de l'émetteur sera rejeté.

En cas de rejet de la requête du client car les k-1 autres clients ne sont pas trouvés, on peut évaluer le système comme étant peu fiable. En outre, certains systèmes de m-business ne peuvent pas tolérer l'expansion de la région et le retard temporel compromet la précision des Qos et la réponse.

Contrairement aux travaux précédents, dans notre contribution, nous allons aborder la protection de la vie privée de l'emplacement et la vie privée des requêtes de clients en même processus de protection. En plus, afin d'assurer la fiabilité de notre travail, nous allons proposer une approche qui traite toutes les requêtes des clients, autrement dit, il n'existe pas des cas de rejet des requêtes dans notre approche, nous veillerons à cela en créant des Dummies.

En fait, les approches précédentes ont fourni des solutions particulières contre un seul type quelconque d'attaque. Par conséquent, dans ce travail, nous proposons une approche de protection qui prend en compte des séries d'attaques dans le même processus de protection de la vie privée de client (attaque de localisation, attaque de suivi, attaque de liaison, attaques d'échantillonnage de requête et attaque d'homogénéité). Comme particularité de notre contribustion, elle traite une série d'attaques dans le même processus de camouflage.

5.3 Contexte et problématique

L'utilisation des applications m-business, peut entraîner deux types de problèmes de vie privée. Le premier est que l'attaquant peut accéder aux données de l'emplacement d'origine de l'utilisateur et en obtenant des informations personnelles relatives à la vie privée de l'utilisateur à l'aide des données collectées. L'autre est que le fournisseur de services non fiable peut obtenir les informations personnelles sensibles de l'utilisateur

en analysant le contenu des requêtes et les données de localisation exactes reçues, et même revendre ou divulguer les informations de la vie privée à but lucratif.

Par conséquent, la vie privée de l'emplacement (Location Privacy) peut être définie comme la capacité d'empêcher les parties non autorisées d'apprendre l'emplacement actuel ou passé, il est également un type particulier de la vie privée de l'information [133]. La vie privée de l'identité de l'utilisateur consiste à empêcher la divulgation des requêtes de l'identificateur d'identité de l'utilisateur lorsque l'attaquant obtient et analyse les autres renseignements liés à l'identité de l'utilisateur. Par exemple, les informations de l'emplacement peuvent être utilisées comme une pseudo-identité dans la requête [134].

Par ailleurs, la protection de la vie privée de la requête (Query Privacy) est une partie importante de la protection de la vie privée dans le m-business fournissant les services de LBS, et son but est d'empêcher les adversaires de lier le contenu de la requête à un utilisateur spécifique [135].

Pour préserver la vie privée, l'emplacement exact des utilisateurs qui envoient des requêtes aux fournisseurs LBS ne doit pas être divulgué. Au lieu de cela, les données de localisation sont d'abord perturbées ou cryptées. Par exemple, pour empêcher l'identification des utilisateurs, certaines travaux existantes génèrent quelques des endroits fictifs aléatoires et d'envoyer un certain nombre de requêtes redondantes aux fournisseurs [81], [82].

Notre objectif est de proposer une approche qui permet de protéger de la vie privée de client mobile lorsque les emplacements des clients sont continuellement mis à jour (c.-à-d. la vie privée de l'emplacement des requêtes continues a été prise en compte). En plus, nous avons pris en compte des mouvements des clients mobiles (comme les caractéristiques de vitesse et de direction) [131].

5.4 Préliminaires

Dans cette section, nous présentons quelques définitions des concepts utilisés dans notre contributions.

Définition 01 (L'information d'emplacement IE)

L'information d'emplacement est l'empreinte des clients en forme (x : la latitude, y : la longitude de l'emplacement du client), ces valeurs peuvent être déterminées par le GPS ou d'autres composants de positionnement.

Définition 02 (La Requête de client mobile Q_{CM})

La requête de client mobile Q_{CM} se compose de : $Q_{CM} = \{C_{id}, P, IE, T, bsns\}$, Où : C_{id} est l'identité du client mobile, P représente le profil d'exigence de vie privée de client mobile (K, A_{min}, A_{max}, T) comme détaillé ci-dessous (définition 14). IE est l'information d'emplacement, $T = (T_s, T_{exp})$: est l'horodatage où T_s représente le temps à laquelle la requête est créée et T_{exp} est le délai d'expiration de la requête. En plus,

$(T_{exp} - T_s)$: peut être utilisé pour déterminer le nombre d'instantanés dans la requête continue. *bsns* : le contenu de la requête (l'information ou un service demandée par le client mobile).

Définition 03 (La requête Continue)

Une fois qu'un client mobile CM envoie une requête au serveur d'anonymisation **AS**, ce dernier (AS) continue d'émettre la requête à différents intervalles de temps au nom de client jusqu'à ce que la requête soit expirée. Une requête continue peut avoir l'un des trois états :

- **Fresh** : Une requête nouvellement créée à Ts s'appelle une *nouvelle requête*.
- **Actif** : est la requête qui a été amorcée auparavant et non terminée et qui active pendant la période de $T_{exp} - T_s$.
- **Expiré** : une requête active est expirée lorsque le temps T_{exp} atteint.

Définition 04 (La région de camouflage R)

L'emplacement exact du client mobile est prolongé en tant que région rectangulaire (ou circulaire) qui comprend l'émetteur de la requête et k-1 autres clients.

Définition 05 (L'anonymat d'emplacement, Location k-anonymity)

Au début des années 2000, Latanya Sweeney [45], a proposé une méthode, nommée k-anonymat, pour prévenir les ré-identifications via des croisements de données. Puis en 2003, Gruteser et al [64], incorporent le mécanisme de k-anonymat pour protéger la vie privée de l'emplacement de client. Le mécanisme de k-anonymat se réfère à la situation où pour chaque client il y a au moins k-1 autres clients qui utilisent d'emplacement semblable.

Définition 06 (La granularité de camouflage)

La région camouflée (cacher, masquée) doit être plus grande que la valeur de seuil spécifiée par le client mobile A_{min}.

Définition 07 (une clique)

Soit $G = (V, E)$ un graphe non dirigé où V est un ensemble de nœuds représentant les localisations des clients mobiles qui ont soumis des requêtes, et E est un ensemble d'arêtes (bords). Soit une clique $C = (S, A)$ de G où, S est un ensemble de nœuds de clique ($S \subseteq V$) et A est un ensemble d'arêtes de clique ($A \subseteq E$).

Une clique C d'un graphe non orienté $G = (V, E)$ est un sous-ensemble des sommets ($S \subseteq V$) de ce graphe dont le sous-graphe induit est complet, c'est-à-dire que deux sommets quelconques de la clique sont toujours adjacents, le nombre d'arêtes de C doit être $w * (w - 1)/2$, où w est le nombre de sommets dans S.

Définition 08 (La requête de serveur d'anonymisation)

La requête de ce serveur se compose de $S_Q = P_{id}, R, it, bsns$, où P_{id} est le pseudonyme du client, R est la région de camouflage, it est l'intervalle de temps (cet intervalle se compose de : T_s est l'heure à laquelle la requête est créée et T_{exp} est le délai d'expiration de la requête) et le *bsns* est les informations demandé par le client. Pour

la requête continue, la requête sera périodiquement publiée par **AS** dans la période (T_{exp} – T_s). En plus, on peut utiliser (T_{exp} – T_s) pour déterminer le nombre d'instantanés n (***Snapshots***) dans la requête continue. En général, plus la requête active dure longtemps, plus le nombre d'instantanés est grand.

Définition 09 (La propriété de réciprocité, K-Sharing)

La propriété de réciprocité est définit comme suit :

- ✓ la région de camouflage doit contenir l'émetteur de la requête et au moins (k-1) autres utilisateurs supplémentaires.
- ✓ la région de camouflage doit partager aussi par au moins k de ces utilisateurs.

Définition 10 (Limite maximale du mouvement MMB et Limite maximale d'arrivée MAB)

La limite maximale du mouvement (MMB_{CM}, t_i, t_{i+1}) de client CM à t_i est rectangle (ou cercle) qui étend la région de camouflage en t_i (R_CM, t_i) par un rayon de **r**. Ceci est calculé comme suit : $r = V_{CM} * (t_{i+1} - t_i)$, où V_{CM} est la vitesse maximale du client (par exemple, la limite de vitesse de la route).

La limite d'arrivée maximale (MAB_{CM}, t_{i+1}, t_i) de client CM à t_{i+1} est rectangle (ou cercle) qui étend la région de camouflage en t_{i+1} (R_{CM}, t_{i+1}) par un rayon de **r**, où $r = V_{CM} * (t_{i+1} - t_i)$.

Définition 11 (La limite de la région de camouflage MBR)

L'algorithme de camouflage devrait avoir une qualité relativement bonne. Par conséquent, la zone de camouflage Z est introduite. Si R_t est une région de camouflage et EC_t est l'ensemble de clients camouflés dans R_t au temps t, la zone de camouflage Z de R_t est définie comme suit :

$$Z = \{Max(x) - Min(x)] * [Max(y) - Min(y)\} \tag{5.1}$$

Où, max (x), min (x), max (y), min (y) sont la valeur maximale et minimale de latitude et de longitude de l'emplacement du client dans EC_t.

Définition 12 (Paramètre de vie privée : anonymisation locale et globale)

Dans notre système, l'utilisateur peut définir ses propres paramètres de vie privée, car ceux-ci peuvent être très différents en raison de la diversité des clients et des occasions, qui peuvent être transmis au serveur d'anonymisation en même temps que la requête :

- ✓ ***Anonymisation locale*** k_{local} ***:*** il montre qu'au moins $k_{local} - 1$ autres utilisateurs doivent être masqués avec le client de requête dans le premier instantané. Donc la probabilité de découvrir l'emplacement exact est inférieure à$1/k_{local}$. En plus, ce paramètre est la contrainte d'anonymat locale pour les requêtes. Nous utilisons la contrainte k_{local} pour garantir que chaque instantané individuel est anonyme en ce qui concerne une certaine valeur de K (***Local privacy***). Nous utilisons ce paramètre pour le premier instantané (***the first snapshot***).

✓ ***Anonymisation globale*** K_{global} ***:*** est le niveau d'anonymat global qui assure l'accumulation de tous les instantanés soumis est aussi anonyme en ce qui concerne un certain k_{global} (***Global privacy***). La taille de l'intersection de l'ensemble de camouflage actuel avec ceux générés précédemment doit être supérieure à k_{global} afin de garantir une confidentialité globale. Même si les adversaires possèdent tous les ensembles de camouflage, ils ne peuvent pas distinguer le client mobile (l'émetteur de la requête) à partir d'au moins $k_{global} - 1$ autres. L'exigence de K_{global} peut résister à l'attaque de suivi des requêtes (*the query tracking attack*).

Définition 13 (la similarité de vitesse, la direction et l'accélération)

Soit $V_i = (vi_x, vi_y)$ et $A_i = (ai_x, ai_y)$ les vecteurs bidimensionnels du client i, la similarité de la vitesse $Sim_V(i, j)$ et la similarité d'accélération $Sim_A(i, j)$ du client i et j peuvent être calculés comme suit :

$$Sim_V(i,j) = \sqrt{(vi_x - vj_x)^2 + (vi_y - vj_y)^2} \tag{5.2}$$

$$Sim_A(i,j) = \sqrt{(ai_x - aj_x)^2 + (ai_y - aj_y)^2} \tag{5.3}$$

Où, nous considérons deux clients i, j avec l'emplacement $IE(xi, yi)$ et $IE(xj, yj)$ avec deux angles de direction θ_i et θ_j respectivement à un emplacement d'origine $IE(xo, yo)$, et $\triangle y = yi - yo$ et $\triangle x = xi - xo$. Leur similarité directionnelle θ_{sim} peut être calculée comme indiqué dans [136] :

$$\Theta_{sim}(i,j) = |\Theta_j - \Theta_i| \tag{5.4}$$

$$\Theta_i = tang^{-1}\frac{\triangle y}{\triangle x} \tag{5.5}$$

où, $\triangle y = y_i$- y_o et $\triangle x = x_i$ - x_o.

Définition 14 (le profil d'exigence de vie privée)

Dans notre contributions, nous avons pris également en compte le profil d'exigence de vie privée des clients, où le client peut définir son profil (paramètres de vie privée) ce qui lui permettra de déterminer son exigence minimale de vie privée de ses choix à différents emplacements. Par exemple, un client malade peut vouloir un niveau de confidentialité plus élevé au centre de cancérologie que dans un centre commercial. Ces paramètres peuvent être livrés au serveur d'anonymisation **AS** avec la requête :

✓ **K :** représente le niveau d'anonymat de l'emplacement, pour cela nous utilisons le modèle de k-anonymat afin de garantir l'anonymat ***local*** et ***global*** (Définition 12).

✓ (A_{min}, A_{max}) : Ces paramètres précis la superficie minimale et maximale qu'une région de camouflage devrait avoir. On utilise Amin afin d'empêcher la région de

camouflage d'être trop petit pour les zones très peuplées et Amax, afin d'empêcher la région de camouflage d'être trop grand pour améliorer la QoS.

✓ **T :** C'est le délai maximum tolérable de camouflage. En plus, le temps est un paramètre de QoS, plus la valeur de **T** est grande, plus la QoS est mauvaise. Puisque le client aura plus de chance de s'éloigner de l'emplacement où la requête a été émise.

Définition 15 (Les propriétés d'ensemble candidat de camouflage EC)

L'ensemble de client mobile est un ensemble candidat de camouflage EC si et seulement si pour tous les clients $CM \in EC$ doivent être respectés les propriétés Cs principales suivantes :

✓ Les clients de l'ensemble de camouflage doivent être sous la forme de la ***Clique*** (Définition 07).

✓ les clients de la région camouflée doivent avoir des vitesses et l'accélération similaires et se déplacent dans des directions similaires (Définition 13), c.à.d. les clients qui sont camouflés ensemble doivent être relativement proches de la distance pour avoir la région camouflée effective relativement petite et par conséquent une bonne QoS. Ainsi que les distances entre les nœuds mobiles sont considérés pour chaque instantané (**Snapshot**) de camouflage.

✓ $|EC| >= k_{cm}$ l'anonymat de l'emplacement selon le modèle de k-anonymat afin de protéger la vie privée de l'identité de client et le contenu de la requête.

✓ la granularité du camouflage afin d'améliorer la QoS, la région camouflée doit satisfaire la superficie minimale et maximale $A_{min} <= MBR(EC) <= A_{max}$

✓ Pour faire face à l'attaque d'homogénéité (si tous les clients de la région camouflée ont demandé le même service), nous devons assurer la propriété de l-Diversity (nous diversifions les requêtes).

Définition 16 (Les critères de la région de camouflage qualifiée)

Le **MBR** (*Minimum Bounding Rectangle*) de l'ensemble candidat de camouflage EC_{ti} (définition 15) en t_i est une région candidate de camouflage CR_{ti}, nous nous référons à la région de camouflage précédente de chaque client (en $ti-1$) par R_{cm}, t_{i-1}.

Par conséquent, la région candidate de camouflage (CR_{ti}) doit satisfaire toutes les conditions d'EC_{ti} (définition 15).

Ensuite, si la région candidate de camouflage CR_{ti} remplit les conditions préalables suivantes alors CR est une région de camouflage qualifiée R_{ti} :

✓ la distance entre les régions de camouflage en t_i et t_{i-1} doit respecter la distance de **Hausdorff** pour faire face à l'attaque de l'emplacement.

✓ Pour les requêtes continues, il faut que la taille de l'intersection de la région candidate de camouflage CR_{ti} avec ceux générés précédemment doit satisfaire

l'exigence de l'anonymisation globale K_{global} (Définition 12) :

$$|CR \cap CR_1 \cap CR_2 \cap \cdots \cap CR_{t_{i-1}}| \geq K_{global} \tag{5.6}$$

✓ La région masquée R_{ti} doit satisfaire à la propriété de $k - sharing$ (Définition 09) et EC est un ensemble de clients mobiles de région de camouflage R.

Comme une région de camouflage plus grande indique une distorsion de données plus élevée, nous introduisons les paramètres A_{min} et A_{max} pour réduire la distorsion des données en cas de la QoS est mauvaise et pour assurer que la région de camouflage n'est pas trop petite ou trop grande dans une zone peuplée.

Après la construction de la région de camouflage R_{ti}, l'**AS** redirige la requête de la région de camouflage R_{ti} (requête transformée Définition 18) au lieu du contexte d'emplacement exact vers les fournisseurs de services, où la demande est traitée (Definition 08). Pour faire l'équilibre entre la vie privée et la Qos, nous combinons les paramètres A_{min} et A_{max} avec k_{local} et k_{global}.

Définition 17 (Modèle de graphe)

Dans notre contributions, les exigences de vie privée spécifiées par le client sont modélisées par un Graphe $G(V, E)$ non orienté. Ainsi, les ensembles de camouflage sont déterminés à l'aide de la recherche des cliques dans le graphe. On utilise le modèle de graphe pour faciliter le camouflage de région.

Soit $G(V, E)$, un graphe non orienté où V est un ensemble de nœuds représentant les clients mobile (ou bien les emplacements de client) qui ont soumis les demandes de requête basées sur l'emplacement (location-based query requests), et E est un ensemble d'arêtes.

Afin de construire le graphe, nous utilisons la distance de **MMB** (définition 10) afin de déterminer les voisins et construire les arêtes entre les clients mobiles. Pour chaque client, les voisins sont ceux dont le **MMB** est contenu l'une dans l'autre, autrement dit, il existe un arc eps entre deux clients $C1$ et $C2$, si et seulement si :

- $C1 \neq C2$, (ils ont différents pseudonymes)
- $C1$: est couvert par MMB_{C2,t_{i-1},t_i}
- $C2$: est couvert par MMB_{C1,t_{i-1},t_i}

Nous utilisons le modèle de graphe pour faciliter la recherche des cliques (Définition 07), une fois qu'une clique (k nœuds) est trouvée, tous les clients au sein de la clique peuvent former un ensemble candidat de camouflage EC_{ti} et le **MBR** de leurs emplacements peut être utilisé comme la région candidat de camouflage CR_ti (Définition 15 et 16).

Ensuite, pour chaque client $CM \in EC_ti$, on calcule leur $d_{haus}(R_{t_{i-1}}, CR_{t_i})$. Si la propriété **MAB** (Définition 21) est violée, on étend la région CR_ti jusqu'à ce que le nouveau **MAB** couvre la région $R_{t_{i-1}}$.

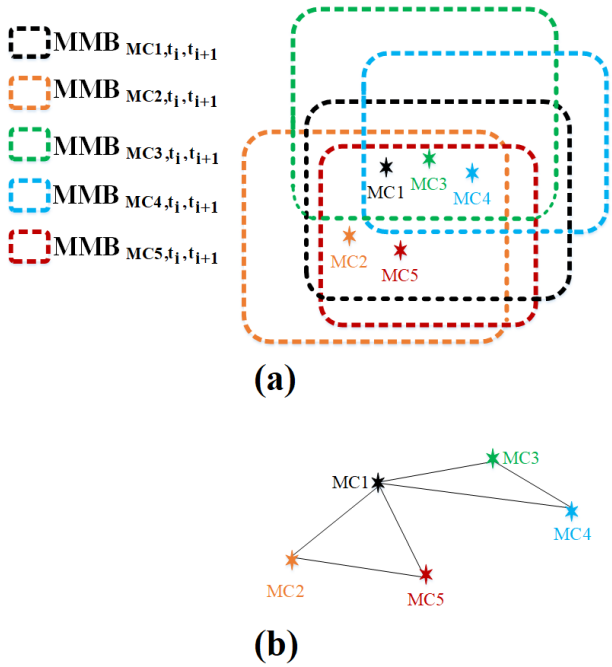


FIGURE 5.1 – Illustration du modèle de graphe.

Définition 18 (La requête de région Ri)

La requête de région Ri est formée de trois parties R_{id}, ER_i, CR_i. Où, R_{id} est l'attribut d'identification d'une région, ER_i est l'ensemble des requêtes dans R_i, et CR_i est le rectangle à limite minimum (**MBR**) couvrant toutes les requêtes de région R_i.

Nous utilisons aussi, $|R_i|$ pour définir le nombre de clients en ER_i. Par conséquent, la requête de région $(R_i, bsns)$ remplacera la requête de client demandeur Q_{CM} et sera transmise aux fournisseurs de services pour générer les résultats. Si un client mobile CM n'a pas émis de requête avant, la dernière région camouflée est définie comme étant la totalité de la zone de service afin que son **MMB** puisse couvrir tous les nœuds (clients) existants.

Définition 19 Evaluation (K_{global}, n)

Étant donné une requête continue, K_{global} représente la taille de l'intersection de toutes les régions camouflées avec succès consécutivement. Le nombre maximal de régions camouflées répondant aux les exigences de vie privée et de qualité dans les instantanés continus est noté **n**.

Pour un algorithme particulier, K_{global} plus grand signifie une meilleure préservation de la vie privée et la valeur maximale de K_{global} est le nombre de clients dans la région initiale $|R1|$. Sans considérer T_{exp}, **n** devrait être aussi grand que possible (être infini dans les conditions idéales). Les deux peuvent être utilisés pour mesurer la performance des algorithmes de camouflage (cloaking algorithms). On dit qu'un algorithme de cloaking est efficace pour la protection contre les attaques s'il maintient autant que possible les clients de région initiale R_1.

5.5 Modèles d'attaques

5.5.1 Propriétés d'attaque

Toute partie possédant les connaissances suivantes peut être un attaquant potentiel :

- ✓ Historique : un ensemble de régions camouflées avec succès consécutivement (dans un temps continu).
- ✓ La vitesse maximale de client mobile (Speed Road), qui peut être déduite de la limite de vitesse de la route et/ou le type client. Par exemple, dans le cas de client conduit, la vitesse ne doit pas dépasser 150 km/h ; et dans le cas le client marche, la vitesse ne peut pas être supérieure à 5 km/h.
- ✓ Les emplacements des clients mobiles qui envoient les requêtes.

5.5.2 Attaques de localisation continues

Pour les requêtes continues, les utilisateurs mobiles doivent continuellement signaler leurs informations de localisation à un serveur **TTP**, et les résultats de la requête seraient continuellement retournés pour une période de temps désignée (appelée durée de vie de la requête). L'idée générale d'une attaque à plusieurs positions (***continuous location attacks***) est qu'un attaquant suit et corrélait plusieurs mises à jour de position ou requêtes d'un utilisateur afin de réduire la vie privée de l'utilisateur.

La plupart des algorithmes existants (exemples, [9], [64], [15], [137]), qui respectent le modèle de k-anonymat, ne concernent que les emplacements des utilisateurs instantanés (snapshot location attacks). Ils n'ont pas pris en compte l'effet des mises à jour continues de l'emplacement. Cela peut conduire à de graves violations de la vie privée lorsque différentes requêtes ponctuelles sont fréquemment émises par un utilisateur mobile. Dans notre solutions nous nous somme intéressé par les attaques de localisation continues.

Si un attaquant (par exemple, le fournisseur de services) peut recueillir historiques de camouflage (les régions camouflées) d'un utilisateur ainsi que le modèle de mobilité (par exemple, limite de vitesse), la vie privée de l'emplacement de l'utilisateur peut être compromise.

De plus, notre solutions traite d'une série d'attaques dans le même processus de camouflage (attaque de localisation, attaque de suivi, attaques d'échantillonnage de requête et l'attaque d'homogénéité).

5.5.2.1 Prévenir l'attaque d'emplacement

Ici, nous présentons la définition formelle de l'attaque d'emplacement.

Définition 20 (la définition formelle des attaques d'emplacement)

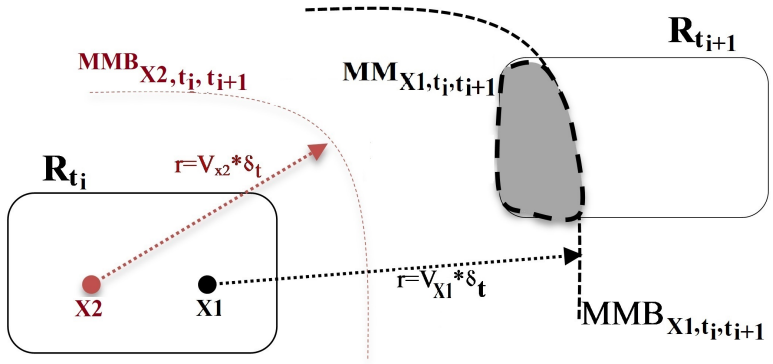


FIGURE 5.2 – Modèle d'attaque lorsque le client se déplace.

Nous nous référons à la zone d'intersection entre $R_{CM,t_{i+1}}$ et $MMB_{CM,ti,t_{i+1}}$ par $MM_{cm,ti,ti+1}$, où, **MMB** et **MAB** sont calculés comme indiqué dans la définition 10 et :

$$MM_{MC,t_i,t_{i+1}} = MMB_{MC,t_i,t_{i+1}} \cap R_{MC,t_{i+1}} \tag{5.7}$$

En outre, Nous nous référons à la zone d'intersection entre R_{MC,t_i} et MAB_{MC,t_{i+1},t_i} par MA_{MC,t_{i+1},t_i}, où :

$$MA_{MC,t_{i+1},t_i} = MAB_{MC,t_{i+1},t_i} \cap R_{MC,t_i} \tag{5.8}$$

où, $MM_{MC,t_i,t_{i+1}}$ et MA_{MC,t_{i+1},t_i} sont illustrés dans la figure 5.4.

Pour tout t_i et $ti + 1$, si une inégalité de ($MM_{MC,t_i,t_{i+1}} \neq R_{MC,t_{i+1}}$) ou ($MA_{MC,t_{i+1},t_i} \neq R_{MC,t_i}$) alors la vie privée d'emplacement de client mobile CM pourrait être compromise. Cette attaque est nommée comme l'attaque de l'emplacement.

Par exemple dans la figure 5.2 montre le modèle d'attaque lorsque client se déplace. On suppose qu'il y a deux régions de camouflage R_{t_i} et $R_{t_{i+1}}$ qui sont signalées par le client mobile CM_A aux horodatages t_i et t_{i+1}, respectivement, où V_{CM} est la vitesse maximale de client, et $\delta_t = \mid t_{i+1}$ - $t_i \mid$.

L'attaquant peut essayer d'élaguer les parties de R_{t_i} et $R_{t_{i+1}}$ pour identifier le client de deux façons :

— **Par l'utilisation de MMB :** Déterminer s'il y a un emplacement $x \in R_{t_i}$ dont le client ne peut pas atteindre un certain emplacement $y \in R_{t_{i+1}}$, même en se déplaçant à la vitesse maximale V_{CM}. Formellement, une attaque est réussie ssi :

$$\exists x \in R_{t_i}, \forall y \in R_{t_{i+1}}, d(x, y) > V_C \times \delta_t \tag{5.9}$$

Dans la figure 5.2, un client qui se déplace du point x_1 est capable d'atteindre un point dans la région hachurée de $R_{t_{i+1}}$ dans le temps δ_t. Cependant, si l'em-

placement initial de CM_A était x_2, atteindre $R_{t_{i+1}}$ n'aurait pas été possible. Par conséquent, un attaquant peut exclure un sous-ensemble de R_{t_i} comme position possible pour le client, donc la vie privée est violée [118].

— **Par l'utilisation de MAB :** Déterminer s'il existe un emplacement $y \in R_{t_{i+1}}$ que le client ne peut pas atteindre d'un certain emplacement initial $x \in R_{t_i}$, même en voyant à vitesse maximale V_{CM}. Formellement, une attaque réussit ssi :

$$\exists y \in R_{t_{i+1}}, \forall x \in R_{t_i}, d(x, y) > V_{CM} \times \delta_t \tag{5.10}$$

Pour empêcher les violations de la vie privée de client mobile, il est nécessaire de s'assurer qu'aucune des équations 5.9 et 5.10 ne soit jamais vérifiée. En d'autres termes, il est nécessaire d'assurer la réalisation des équations 5.7 et 5.8 de la définition 20 ($MM_{MC,t_i,t_{i+1}} = R_{MC,t_{i+1}}$) et ($MA_{mc,t_{i+1},t_i} = R_{MC,t_i}$). Autrement dit, il faut assurer les propriétés MMB et MAB (Définition 21). C'est-à-dire que les propriétés MMB et MAB de la distance de Hausdorff (Eq 5.13 et 5.14 de la définition 21) doivent être garanties.

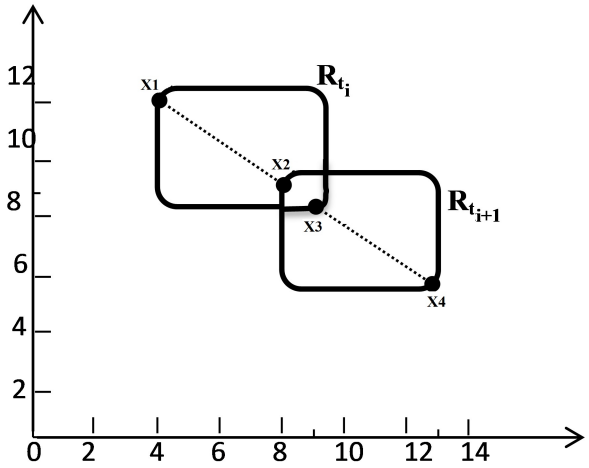


FIGURE 5.3 – Distance de Hausdorff [118].

Définition 21 (Distance d'Hausdorff et propriétés du MMB et du MAB)
Pour définir l'ensemble de camouflage EC, nous avons besoin d'utiliser la distance d'Hausdorff. Soit R_{t_i} et $R_{t_{i+1}}$ deux régions de camouflage, p et q deux clients mobile ($p \in R_{t_i}$ et $q \in R_{t_{i+1}}$), la distance de Hausdorff est donc définie comme suit :

$$d_{haus}(R_{t_i}, R_{t_{i+1}}) = \max\{h(R_{t_i}, R_{t_{i+1}}), h(R_{t_{i+1}}, R_{t_i})\} \tag{5.11}$$

où,

$$h(R_{t_i}, R_{t_{i+1}}) = \max_{p \in R_{t_i}} \min_{q \in R_{t_{i+1}}} Distance(p, q) \tag{5.12}$$

$Distance(p, q)$ représente la distance entre deux clients mobile p et q. Par exemple, dans la figure 5.3, $d_{haus}(R_i, R_j) = \mid X1\ X2 \mid = \sqrt{25}$, et $d_{haus}(R_j, R_i) = |X4X3| = \sqrt{20}$.

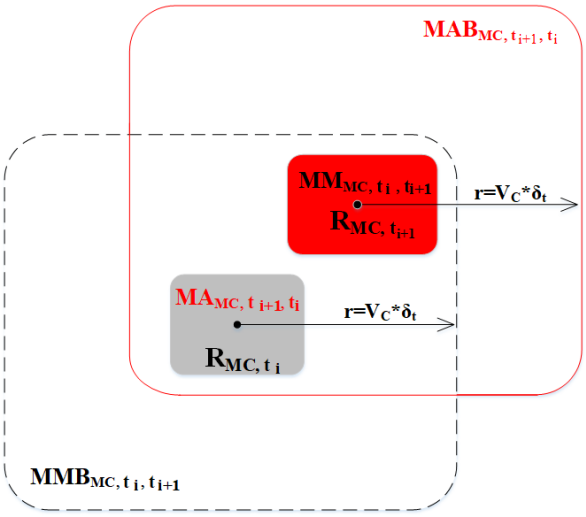


FIGURE 5.4 – Propriétés MMB et MAB.

Par conséquent, les propriétés suivantes doivent être assurées pour empêcher l'attaque de l'emplacement :

✓ **Propriété MMB :** la région $R_{t_{i+1}}$ doit être entièrement couverte par $MMB_{MC,t_i,t_{i+1}}$ comme illustré dans la Figure 5.4, ce qui indique :

$$d_{haus}(R_{t_i}, R_{t_{i+1}}) \leq V_C \times \delta_t \tag{5.13}$$

✓ **Propriété MAB :** et en plus, la région R_{t_i} doit être entièrement couverte par MAB_{MC,t_{i+1},t_i} comme illustré dans la Figure 5.4, ce qui indique :

$$d_{haus}(R_{t_{i+1}}, R_{t_i}) \leq V_C \times \delta_t \tag{5.14}$$

5.5.2.2 Prévenir l'attaque de requête (Query attack)

Un adversaire peut lancer une attaque de suivi des requêtes (query tracking attack) en calculant $R_{ti} \cap R_{ti+1}$ lors de l'obtention de la région de camouflage du client CM à ti et t_{i+1} pour réduire la région de camouflage. Voici l'exemple de l'attaque de suivi des requêtes et l'attaque d'échantillonnage de requêtes :

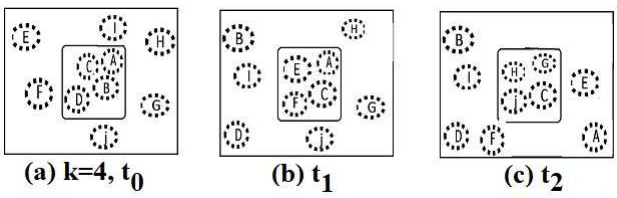


FIGURE 5.5 – Exemple d'une attaque de requête.

Comme le montre la figure 5.5, les régions de masquage de client C à trois horodatages différents $(t_0; t_1; t_2)$ sont représentés par les rectangles avec des lignes continues. Si un adversaire a l'historique de cloaking, il peut alors calculer l'intersection de tous

les ensembles de masquage. Il peut donc en conclure que le client C est celui qui a soumis la requête.

L'exigence de l'anonymisation globale K_{global} (Définition 12) et la propriété de $K - Sharing$ (Définition 09) doivent être remplie pour empêcher l'attaque de tracking et l'attaque d'échantillonnage de requête. Les détails des attaques (attaque de suivi, attaque d'échantillonnage de requête et attaque d'homogénéité) sont présentés dans le chapitre 03.

5.6 Approche proposée

Dans cette section, nous présentons notre approche. Les principales contributions de notre approche sont les suivantes :

- ✓ Une nouvelle approche de protection de la vie privée de client mobile basé clique est proposée en tenant compte des mouvements des clients mobiles comme les caractéristiques de vitesse et direction.
- ✓ Les travaux actuels définissent séparément la vie privée de l'emplacement et la vie privée de la requête. Pour cette raison, dans notre approche, nous nous concentrons sur la protection de la vie privée de l'emplacement et la protection de la vie privée de la requête de client dans le même processus de camouflage contre les fournisseurs de services. Puisque les clients mobiles ne veulent pas divulguer (révéler) leurs emplacements et/ou leurs requêtes aux fournisseurs de services. Les résultats d'analyse montrent que l'algorithme peut obtenir un **bon équilibre** entre **QoS** et **la vie privée** ;
- ✓ Nous utilisons le principe de clique (Définition 07), parce que les cliques peuvent être rapidement identifiées et utilisées pour générer la région de camouflage lorsqu'une nouvelle requête arrive.
- ✓ Notre algorithme satisfait la propriété de K-Sharing (définition 09), pour faire face aux attaques.
- ✓ Dans notre approche, toutes les requêtes reçoivent une réponse même si k-1 autres utilisateurs ne sont pas disponibles, car nous générons des différents mannequins réels (Dummies) au lieu de supprimer la requête.
- ✓ Pour assurer l'équilibre entre la vie privée des clients et la qualité de service fournies par les fournisseurs de services, nous adoptons la solution la plus simple et la plus récente ce qui est le camouflage de l'emplacement. Le camouflage d'emplacement masque l'emplacement du client dans une région de camouflage R.

5.6.1 Architecture du système

Dans notre solution, nous adoptons l'architecture de tiers de confiance **TTP** composée de clients mobiles, Serveur d'anonymisation (**AS**) et les fournisseurs de LBS (**FS**) comme illustré dans la figure 5.6. L'objectif principal de notre travail est la protection la vie privée de client (la localisation et la requête) en utilisant le camouflage spatial et temporel basé sur le modèle de k-anonymat. Notre travail a l'avantage de traiter une série d'attaques de vie privée de client dans le même processus de camouflage.

Généralement dans les applications de business mobiles, l'information demandée par le client mobile est directement transmise comme une requête à l'AS, où la requête est traitée et camouflée avec les autres. Les fournisseurs FS est l'endroit critique où la vie privée des clients peut être violée par **le contexte d'emplacement** et **le contenu de la requête**. Afin de protéger la vie privée de client mobile ainsi que la QoS, cette architecture se base sur une entité appelée Serveur d'anonymisation (**AS**) entre l'application m-business et le FS. La figure 5.6 illustre l'architecture de notre système.

Dans les paragraphes suivants, nous allons présenter en détail les composants principaux dans notre architecture :

- **Les Fournisseurs des services FS :** sont des serveurs qui offrent les informations et des services à base d'emplacement aux clients, ces serveurs ne sont pas dignes de confiances. Nous supposons que le FS est l'adversaire et qu'il est capable d'obtenir des informations globales et surveiller les requêtes envoyées par les clients.
- **Le Serveur d'anonymisation AS :** est un serveur qui agit comme un broker (un tiers de confiance) pour gérer les communications entre le client mobile avec le **FS**. Le rôle principal d'**AS** est la transformation spatiale et temporelle, *c.-à-d.,* l'emplacement exact des clients est transformé à une région de camouflage R et l'horodatage original T est transformé en l'intervalle de temps it. De plus, nous supposons que le serveur d'anonymisation **AS** est approuvé, sauf si les clients perdent le contrôle physique sur lui.
- **Le Client Mobile CM :** est l'émetteur de requête, où la requête émis par le client est envoyée au **FS** par **AS**.

Le noyau de notre système est le serveur **AS** qui crée la région de camouflage basé ***clique*** (Définition 07). Le serveur **AS** se compose de quatre parties, à savoir le moteur de camouflage, le raffineur de résultats, le stock de régions camouflées et le stock de profils.

- **Moteur de camouflage :** est responsable de camoufler l'emplacement exact de client dans une région de camouflage contenant au moins $k-1$ d'autres clients et transmet la requête de région aux **FS**.

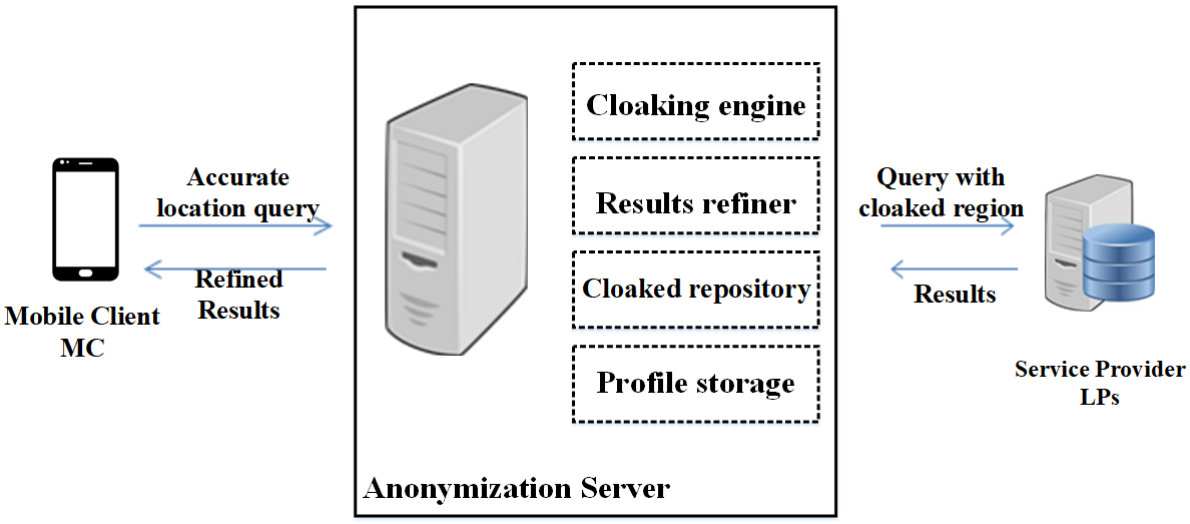


FIGURE 5.6 – Architecture de l'approche.

- **Raffineur de résultats :** filtrer les résultats générés par **FSs** dans un état précis basé sur l'emplacement du client.
- **Stock de régions camouflées :** peut stocker les régions précédemment camouflées et les utiliser pour produire la nouvelle région.
- **Stock de profils :** stocke le profil d'exigence de vie privée de client, y compris les emplacements de préférence pour une vie privée plus élevée.

5.6.2 Fonctionnement de notre approche

Nous supposons que les clients mobiles possèdent la capacité de positionnement, qui peut signaler les emplacements des clients à l'**AS** afin de camouflage. Une autre hypothèse de base pour le fonctionnement de ce système est que les **FS** ne sont pas dignes de confiance et peuvent par accidentellement fuir les contenus des requêtes et les informations de localisation des clients mobiles à d'autres parties comme par exemple un adversaire. Compte tenu d'hypothèses ci-dessus, l'adversaire peut intercepter un ensemble d'échantillons de requêtes transmises aux **FS** et il peut donc être capable de connaître l'emplacement exact et les contenus des requêtes de certains clients mobiles dans la région camouflée. Toutefois, la requête ne doit pas être liée aux clients spécifiques (ce type d'attaque s'appelle ***linking Attack***).

Pour cette raison dans notre travail, nous nous concentrons sur la protection de la vie privée de la localisation (***Location Privacy***) ainsi que la vie privée de la requête continue (***the query linking Privacy***).

Pour les ***requêtes continues***, le serveur **AS** sera périodiquement envoyé la requête aux **FSs** dans la durée de vie de la requête ($T_{exp} - T_s$) avec différentes régions camouflées liées à l'emplacement en temps réel du client jusqu'à l'instant T_{exp} lorsque la requête expire. Pour cela, nous devons satisfaire à l'exigence de K_{global} pour prévenir l'attaque de liaison de requête parce que les régions publiées par **AS** sont différentes.

Maintenant, nous présentons le fonctionnement de notre système :

- Un client mobile CM qui a besoin des services de FS envoie une requête de service (montrant la durée de service) à AS en temps t_1 par une connexion authentifiée et cryptée.
- Lors de la vérification réussie de CM, AS établit un mécanisme de camouflage basé *clique* (comme mentionné en section 5.6.3) pour générer une région de camouflage de l'emplacement de CM avec au moins $k-1$ autres clients mobiles.
- Ensuite, la requête est transmise au processus de camouflage pour générer une région de camouflage R conformément aux exigences de vie privée de client. En plus, le camouflage des clients doit respecter les critères de camouflage qui sont discutées dans des sections précédentes (définition 15 et 16).
- le moteur de camouflage remplace l'identifiant réel de client par un nouvel identifiant de pseudonyme $c_{id'}$.
- Ensuite, si le camouflage a réussi (toutes les conditions de définition 15 et 16 sont remplies), le serveur d'anonymisation AS transmet la requête modifiée $(c_{id'}, R, bsns)$ aux fournisseurs de services. En plus, la requête camouflée est enregistrée dans le stock de régions camouflées sous la forme de $(c_{id}, c_{id'}, P, R_{ti}, t_i)$, où R_{ti} est une région camouflée du client mobile au moment t_i.
- Du côté du fournisseur de services, lors de la réception de la requête avec la région de camouflage $(c_{id'}, R, bsns)$, il recherche tous les résultats qui sont potentiellement des résultats de requête d'un certain emplacement indiquent dans R et retourne tous les résultats à l'**AS**.
- La réponse de fournisseur de services est générique et devrait être filtrée pour obtenir des résultats précis. Le filtrage peut être effectué sur l'**AS** ou par le client mobile.
- Après cela, ces résultats proposés seront raffinés par le serveur **AS** en utilisant l'emplacement exact de client mobile **IE**.
- Ensuite, les résultats nécessaires seront retournés en toute sécurité au client mobile.
- **AS** continuera ensuite à envoyer la requête aux FSs dans la durée de vie de la requête avec différentes régions camouflées liées à l'emplacement en temps réel du client de requête jusqu'à l'instant Texp lorsque la requête expire. Par conséquent, nous utilisons le paramètre d'anonymisation global k_{global}, pour faire face aux attaques de linking.
- Par ce mécanisme, le FS peut seulement savoir du client avec ***le facteur de certitude CF*** de $(1/|R|) * (1/K)$, par conséquent, la possibilité des clients étant attaqués peut être réduite.

5.6.3 Principe de camouflage de notre approche

Dans cette thèse, nous présentons une nouvelle approche de protection de la vie privée du client mobile afin de préserver la vie privée de l'emplacement et des requêtes continues du client mobile pour les applications m-business. Les paragraphes suivants présentent la différence entre notre approche et les approches précédentes [138], [122], [10], [119], [11] :

Le principe de l'approche proposée dans [120] est de continuer à rechercher le même ensemble de clients mobiles jusqu'à ce que la requête expire. Cependant, dans cette l'approche, la région générée doit toujours contenir les clients qui sont membres de la région initiale en t_0. Cette l'approche peut générer d'une large région de camouflage, en raison du mouvement continu des clients. Par conséquent, une large région réduit la qualité des résultats renvoyés par le FS aux clients, ajoute plus de coûts de traitement et de filtrage à l'AS et le client et le serveur AS devient sous charge.

Les techniques proposées dans les travaux [10] et [119] satisfaits que l'anonymat de la région de camouflage actuel et n'assure pas l'anonymat de la région précédente (t_{i-1}). En plus, les auteurs de ces travaux ne considèrent pas la similarité de mouvements des clients (vitesse, direction et le mode de transport de déplacement). En outre, ces travaux présentent une faiblesse dans l'attaque de Linking des requêtes.

La méthode proposée dans [119] peut générer une grande région de camouflage, en raison du mouvement continu des clients. En outre, les auteurs ne prennent pas en compte le critère du temps, car l'intervalle de temps doit être petit, pour garantir la meilleure qualité de recommandation/suggestion des services. De plus, les valeurs de tolérance telles que $\triangle x$, $\triangle y$, A_{min} et A_{max} sont pris par le serveur TTP appelée Location Hider.

L'approche proposée par [122] ne garantit pas la propriété de k-sharing, car les régions camouflées sont différentes. La méthode de découverte des clients les plus proches proposée par [11] augmente la complexité du traitement.

Nous présentons une nouvelle approche de camouflage pour garantir la vie privée de client mobile pour le m-business. Lorsqu'un client mobile veut faire une demande de service aux FSs, il envoie la requête une seule fois au serveur AS. Ensuite, l'AS cache l'emplacement exact de client en utilisant l'algorithme de camouflage qui construit la région de camouflage basée sur la clique de telle sorte que la région de camouflage actuelle située complètement dans le MMB (Définition 10). Puis, le serveur AS continue d'émettre la requête à différents intervalles de temps au nom de client mobile CM (la requête continue) et chaque fois doit tenir en compte l'emplacement du client en temps.

La requête de client sous la forme $Q_{CM} = C_{id}, C, IE, T, bsns$, les paramètres sont expliqués dans définition 02. Pour une nouvelle requête d'un client mobile au temps ti, nous utilisons la distance Hausdorff pour trouver la région sécurisée $R_{CM,ti}$. Par conséquent, l'idée de base de camouflage est de trouver un ensemble de camouflage EC

qui satisfait les conditions de la définition 15.

La méthode de camouflage de notre approche est une stratégie de camouflage par clique, dans laquelle il continue à rechercher les cliques à partir d'un graphe non dirigé jusqu'à ce qu'il trouve une clique comprend le client mobile (le demandeur) avec au moins $k-1$ autres clients les plus proches qui ont des mouvements similaires au demandeur (Définition 13). Dans notre approche, les clients de sous graphe clique représentent l'ensemble candidat de camouflage EC. Par conséquent, l'idée de base du camouflage est de trouver un ensemble candidat de camouflage qui répond aux exigences de la Définition 15. En plus, le rectangle de délimitation MBR (définition 11) entourant l'ensemble de camouflage EC représente la région de camouflage qui sera soumis aux fournisseurs.

Afin de déterminer les voisins pour construire le graphe, chaque fois qu'une requête est émise par divers clients, le serveur AS calcule le **MMB** (définition 10) puis détermine les voisins dont la **MMB** est contenue l'une dans l'autre (définition 17). Après la construction du graphe non orienté, le serveur AS peut déterminer les cliques afin de générer la région de camouflage.

Par conséquent, nous utilisons une clique dans notre approche pour protéger les clients de clique contre les attaques de localisation parce que la clique assure la convergence de la distance entre les clients (Définition 17, la méthode de construction graphe). En outre, les auteurs de [9] ont montré que le problème de trouver des cliques de k-noeuds dans le graphe est équivalent au problème de trouver des ensembles de camouflage satisfaisant k-anonymat de l'emplacement dans un graphe G.

En plus, le serveur AS camoufle l'emplacement exact de client, de telle sorte que la région camouflée actuelle en t_i réside complètement dans le MMB de la région camouflée précédente en t_{i-1} et aussi que la région camouflée précédente en t_{i-1} réside complètement dans le MAB de la région camouflée actuelle en t_i. Ce sont des propriétés très importantes pour faire face aux attaques d'emplacement (nous les appelons les propriétés de MMB et MAB définition 21).

En outre, notre approche de camouflage basé sur l'historique de cloaking, autrement dit, lors de la création de la région de camouflage R_i pour les instantanées suivantes, il faut d'abord considérer les clients les plus proches dans le stock de régions camouflées qui stocke les régions camouflées avec succès préalablement.

En outre, notre approche sépare la vie privée locale K_{local} sur chaque instantané et la vie privée globale K_{global} à travers des instantanés avec des objectifs de vie privée différents (définition 12). De plus, nous exploitons le groupe local d'anonymisation en tant que candidats pour obtenir les candidats du groupe global d'anonymisation comme le montre la figure 5.7.

Où, le demandeur est C et au moment t_0, l'ensemble de camouflage $EC = \{C; A; B; D; H\}$, à l'instant t_1 l'ensemble $EC = \{C; B; D; I; G\}$ et à l'instant t_2 l'ensemble $EC = \{C; A; D; E; I\}$.

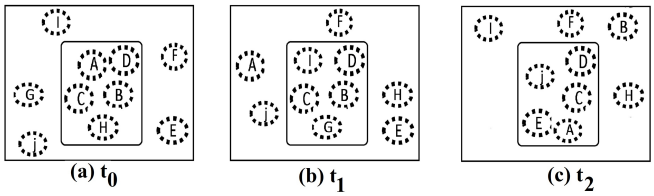


FIGURE 5.7 – Requête de région R_i où $K_{local} = 4$, $K_{global} = 2$.

Pour garantir la vie privée globale, pour chaque instantané de la requête continue, le demandeur MC est caché avec au moins $k-1$ autres clients dans une région masquée. En plus, pour prévenir les attaques (les attaques de tracking, les attaques par échantillonnage de requête et les attaques de l'emplacement.), les $k-1$ autres clients doivent former une clique et avoir des mouvements similaires à ceux du client demandeur.

De plus, dans notre algorithme, le paramètre n représente le nombre total de requêtes instantanées de la région $(R_1...R_n)$ est déterminé par le serveur AS en fonction de l'expiration de la requête T_{exp}. Par conséquent, la période active d'une requête peut être déterminée à partir de $(T_{exp} - T_s)$. Par exemple, pour une requête continue, nous pouvons configurer le serveur AS pour qu'il exécute une requête instantanée toutes les 20 secondes. Par exemple pour une requête avec une période active de 5 minutes, le serveur AS génère 15 régions de camouflage (n = 15) et tente d'exécuter 15 instantanés $(R_1...R_{15})$.

De plus, si la requête du client est récente (premier instantané) et que la condition de Klocal n'est pas remplie, dans ce cas, au lieu de supprimer la requête du client comme dans [10], nous créons différents mannequins réalistes (*Dummies*). Cela est détaillé à la section 5.6.5.

Pour les instantanés suivants dans la durée de vie de la requête continue, l'AS continue à émettre l'instantané aux FS si et seulement s'il peut trouver K_{global} clients mobiles communs à partir de l'intersection avec tous les instantanés précédents. L'instantané qui ne satisfait pas la contrainte K_{global}, nous supprimons cet instantané au lieu de réduire la vie privée globale. De plus, si un instantané est supprimé, l'AS continue de vérifier les instantanés suivants. Par exemple, si la condition de K_{global} est rempli avec R_1 et R_2 et l'AS ne peut pas satisfaire K_{global} avec R_3, il supprime R_3 et continue à vérifier les instantanés ultérieurs $R_4...R_{15}$. De cette manière, l'AS garanti une vie privée globale, mais il peut supprimer certains instantanés (*snapshots*).

5.6.4 Description de l'algorithme

Dans cette thèse, nous introduisons un nouvel algorithme de vie privée intitulé *Mobile Clique Cloak MCC* pour la vie privée de l'emplacement et la vie privée des requêtes continues de client mobile pour les applications m-business. Dans ce travail, nous considérons le camouflage de l'emplacement actuel de client mobile par rapport à

la dernière région camouflée afin de garantir la protection des requêtes continues contre les attaques. En outre, nous permettons au client mobile de choisir leurs exigences de vie privée pour garantir sa vie privée. De plus, notre algorithme considère la similarité des clients dans la vitesse, l'accélération et la direction pour le camouflage afin d'assurer que les requêtes camouflées au moment ti ont une probabilité plus élevée de rester ensemble au moment t_{i+1}.

Dans cette section, nous allons expliquer notre l'algorithme en détail, où algorithme 1 pour une nouvelle requête et algorithme 2 pour une requête active.

Premièrement, si la requête Q_{CM} est récente, nous exécutons l'algorithme 1, où les seuils λ et Θ_{Th} sont déterminés par AS en fonction de l'historique :

Algorithm 1 Procedure for a newly query

Require: the mobile client query $Q_{MC} = \{C_{id}, P, L_i, T, bsns\}$
Ensure: The cloaked region R
1: Discover all clients locations.
2: Find the neighbors by using the MMB of Q_{MC} and of each client in the pre-cloaked set *Pre-clk*.
3: Build the Graph $G = (V, E)$.
4: Find the cliques involving the node representing the requester with their neighbors.
5: Sort these cliques in descending order of clique size in a *Queue-Clique*.
6: **for** each Clique in *Queue-Clique* **do**
7: $Queue\text{-}Vertices \leftarrow Null$, // candidates set
8: Insert Q_{MC} in $Queue\text{-}Vertices$.
9: Insert the vertices of the clique (V) in $Queue\text{-}Vertices$
10: **for** each vertex v' in $Queue\text{-}Vertices$ **do**
11: **if** $(Sim_v(Q_{MC}, v') > \lambda) || (\Theta_{sim}(Q_{MC}, v') > \Theta_{Th})$ **then**
12: Delete v' from $Queue\text{-}Vertices$.
13: **end if**
14: **end for**
15: Find *max-k*, *min-k*, A_{min} and A_{max} of clique.
16: **if** $(MBR(Queue\text{-}Vertices) < A_{min})$ **then**
17: Expand $MBR(Queue\text{-}Vertices)$ until $MBR(Queue\text{-}Vertices) = A_{min}$
18: **end if**
19: **if** $(MBR(Queue\text{-}Vertices) > A_{max})$ **then**
20: Reduce $MBR(Queue\text{-}Vertices)$ until $MBR(Queue\text{-}Vertices) = A_{max}$
21: **if** $(|Queue\text{-}Vertices| < Max(k_{local}, Min\text{-}k))$ **then**
22: Pass to the next clique.
23: **end if**
24: **end if**
25: **if** $(|Queue\text{-}Vertices| >= max\text{-}k)$ **then**
26: **if** $(L\text{-}Diversity = 0)$ **then**
27: $Dem\text{-}Dummies \leftarrow 2$,
28: $Dummies\text{-}Generation(Id_{MC}, Dem\text{-}Dummies, Q_{MC}, MBR(Queue\text{-}Vertices), L_i)$ Call to Algorithm 5
29: **end if**
30: $EC \leftarrow$ the query set of $Queue\text{-}Vertices$
31: $R_0 \leftarrow MBR(Queue\text{-}Vertices)$ //the cloaked region
32: Forward the region request $(P_{id}, R_0, lt, bsns)$ to the LPs , with guarantee the *k-sharing* ; then, the AS updates the graph.
33: **Break**
34: **else**
35: **if** $(|Queue\text{-}Vertices| < Max\text{-}K) ET(|Queue\text{-}Vertices| >= Max(k_{local}, Min_k))$ **then**
36: $Dem\text{-}Dummies \leftarrow Max\text{-}K - |Queue\text{-}Vertices|$
37: $Dummies\text{-}Generation(Id_{MC}, Dem\text{-}Dummies, Q_{MC}, MBR(Queue\text{-}Vertices), L_i)$ Call to Algorithm 5
38: **if** $Rep = True$ **then**
39: Forward the region request $(P_{id}, R_0, lt, bsns)$ to the LPs , with guarantee the *k-sharing* ; then, the AS updates the graph.
40: **Break**
41: **end if**
42: **end if**
43: **if** $(|Queue\text{-}Vertices| < Max(k_{local}, Min_k))$ **then**
44: No candidate, the AS passes to the next clique in a *Queue-clique*.
45: Insert Q_{MC} in the Pre-cloaked *Pre-clk*.
46: **end if**
47: **end if**
48: **end for**

5.6.4.1 Description de l'algorithme 1 :

Lignes 01 à 04 : à l'arrivée d'une nouvelle requête Q_{CM} à t_0, l'algorithme définit l'emplacement IE du client mobile qui a soumis la demande de service. Ensuite, il sélectionne les voisins du demandeur dans l'ensemble pré-masqué (*Pre-clk*). Ensuite, l'algorithme construit un graphe non orienté (définition 17) en utilisant les rectangles MMB de Q_{CM} et pour chaque client dans *Pre-clk*. Ensuite, il essaie de trouver les cliques impliquant le nœud représentant le demandeur Q_{CM} avec ses voisins.

Une fois qu'une clique de k_{local} sommets est trouvée, l'algorithme vérifie si tous les clients au sein de la clique peuvent camoufler ensemble ou non. Afin de répondre à cette question, cet algorithme doit vérifier la similarité des mouvements des clients mobiles de la clique, de sorte qu'il soit nécessaire de prendre en compte la vitesse et la direction (définition 13).

Lignes 05 à 09 : Après la construction du graphe et trouver l'ensemble de cliques, l'algorithme trie les cliques impliquant la nouvelle requête dans un ordre décroissant selon la taille de la clique dans une file d'attente de clique (*Queue-clique*). Ensuite, il commence par la plus grande clique (une plus grande taille). Ensuite, de la clique sélectionnée ; l'algorithme insère les clients de la clique dans une file d'attente de sommets (*Queue-Vertices*).

Lignes 10 à 14 : Après cela, la similarité de vitesse et la similarité de direction sont calculées (Définition 13). Ensuite, seul l'ensemble candidat cloaking ECC (définition 15) répondant à l'exigence de k_{local} et l'exigence relative à la taille de la zone (A_{min}, A_{max}) sont traités comme *une région de camouflage qualifiée* R (définition 16). Ensuite, l'algorithme supprime les clients de la file d'attente *Queue-vertices* qui ne sont pas similaires au demandeur MC. Après cela, nous pouvons classer les clients de la *Queue-vertices* en trois catégories :

- **Candidats actifs :** Si $\mid Queue\text{-}Vertices \mid \geq Max\text{-}k$ et $A_{min} \leq MBR\ (Queue\text{-}Vertices) \leq A_{max}$.
- **Candidats passifs :** Si $\text{Max}(k, Min\text{-}k) \leq \mid Queue\text{-}Vertices \mid < Max\text{-}k$ et $A_{min} \leq MBR\ (Queue\text{-}Vertices) \leq A_{max}$.

  Contrairement aux travaux précédents [10], [11] et [122] afin de transformer les candidats passifs en candidats actifs, nous générerons des Dummies réalistes au lieu de supprimer les clients qui ont un haut niveau de vie privée, (les détails mentionnés à la section 5.6.5).
- **Non-Candidats :** Si $MBR(Queue\text{-}Vertices) < A_{min}$ OU $MBR(Queue\text{-}Vertices) > A_{max}$ OU $\mid Queue\text{-}Vertices \mid < \text{Max}(k, Min\text{-}k)$

Puis, l'algorithme examine toutes les cliques de *Queue-Vertices* jusqu'à ce qu'une clique positive soit trouvée ou transforme la clique négative en une clique positive.

Lignes 15 à 24 : dans ce cas, la région candidate CR_{t_0} est le MBR de *Queue-Vertices*. Ensuite, le serveur AS vérifié la taille de la région MBR ($Queue\text{-}Vertices$), si

elle n'est pas satisfaite, l'AS étend la région CR_{t_i} de tous les côtés jusqu'à ce qu'il soit $MBR(Queue\text{-}Vertices) >= A_{Min}$.

Lignes 25 à 34 : Une fois que toutes les conditions de la similarité et les conditions de la taille de la région MBR sont remplies, le serveur AS doit vérifier les conditions k_{local}-*anonymat*.

$Max_K(Min_k)$ représente la plus haute (basse) valeur de niveau de vie privée de la *Queue-Vertices*. Si la condition de Max_k est remplie (Candidats actifs), l'algorithme peut former un ensemble de camouflage EC_{t_0} et le $MBR(EC_{t_0})$ de leurs emplacements peut être utilisé comme la région de camouflage R_{t_0}.

Lignes 26 à 29 : Si toutes les requêtes de *Queue-Vertices* sont similaires (*L-diversité* =0), le serveur AS diversifie la requête pour éviter l'attaque d'homogénéité. Par conséquent, nous créons le nouveau mannequin (Dummy) (L=2) et le stockons en mémoire.

Lignes 30 à 33 : Ensuite, le serveur AS peut envoyer la demande de région R_{t_0} (Définition 18) aux fournisseurs, à condition que le serveur AS garantisse la propriété *k-sharing* pour la région masquée R_{t_0} (Définition 09). La réalisation de propriété k-sharing est très importante pour faire face aux attaques de requête de type (*Sampling Attack, Query Attack*). Après le succès du processus de cloaking, la région masquée R_{t_0} sera enregistrée dans le stock de région camouflée. Ensuite, le serveur AS met à jour le graphe (il supprime les sommets et les bords de la clique cachée (*Queue-Vertices*)).

Lignes 34 à 42 : Si la condition Max_k n'est pas remplie et ($|Queue\text{-}Vertices| >= Max(K_{local}, Min_k)$), l'algorithme passe à l'étape de la transformation des candidats passifs en candidats actifs en créant les mannequins réalistes (fonction Génération des dummies réalistes), comme mentionné à la section 5.6.5. Ensuite, après la création de dummies ; la région est renvoyée en tant que région camouflée R_{t_0} de l'ensemble de camouflage EC_0. Ensuite, le serveur AS peut envoyer la demande de région R_{t_0} (Définition 18) aux fournisseurs, à condition que le serveur AS garantisse la propriété *k-sharing* pour la région masquée R_{t_0} (Ligne 39, algorithme 1). Après le succès du processus de cloaking, la région masquée R_{t_0} sera enregistrée dans le stock de région camouflée (Ligne 39, algorithme 1). Ensuite, le serveur AS met à jour le graphe (il supprime les sommets et les bords de la clique cachée (*Queue-Vertices*)).

Lignes 43 à 46 : Si ($|Queue\text{-}Vertices| < Max(K_{local}, Min_k)$), dans ce cas aucun candidat, l'AS passe à la clique suivante dans file d'attente de clique *Queue-clique* et insère Q_{CM} dans l'ensemble pré-masqué (*Pre-clk*).

Deuxièmement, si la requête est active, on exécute l'algorithme 2.

5.6.4.2 Description de l'algorithme 2

Lines 01-06 : pour les instantanés suivants (***i***) dans la durée de vie de la requête continue. Un client qui provoque la plus faible distorsion de données est inséré dans la

Algorithm 2 Procedure for an active query

Require: the mobile client query $Q_{MC} = \{C_{id}, P, L_i, T, bsns\}$
Ensure: The cloaked region R
1: $Queue\text{-}common \leftarrow Null$ // the query is active
2: **for** each v' in $(R_1 \cap R_2 \cap ... \cap R_{i-1})$ **do**
3: Find and insert the cliques involving the node representing the requester Q_{MC} with the clients of the previously cloaked regions $(R_1 \cap R_2 \cap ... \cap R_{i-1})$ into $Queue\text{-}common$.
4: **end for**
5: Empty the $Queue\text{-}Vertices$.
6: $Queue\text{-}Vertices = Queue\text{-}common$ with Q_{MC}.
7: Repeat from 10 to 15 (Algorithm 1)
8: **if** $(Queue\text{-}Vertices \cap R_1 \cap R_2 \cap ... \cap R_{i-1} >= K_{global}) and (MBR(Queue\text{-}Vertices) <= A_{max})$ **then**
9: **if** $MBR(Queue\text{-}Vertices) < A_{min}$ **then**
10: Expand R_i until $MBR(Queue\text{-}Vertices) = A_{min}$
11: **end if**
12: $R_i \leftarrow MBR(Queue\text{-}Vertices)$
13: $CR \leftarrow MAB\text{-}Method(Queue\text{-}Vertices)$ Call to Algorithm 3
14: $Rep \leftarrow MMB\text{-}Method(CR, Queue\text{-}Vertices)$ Call to Algorithm 4
15: **if** $Rep = False$ **then**
16: This cloaking process fails.
17: **else**
18: Forward the region request $(P_{id}, R_i, lt, bsns)$ to the LPs , provided that the AS must guarantee the property of *k-sharing*
19: Save the cloaked region R_i in the cloaked repository
20: **end if**
21: **else**
22: The snapshot will be deleted and the cloaking engine will process the following snapshots (or used the previous snapshots).
23: **end if**

file d'attente commune *Queue-common* afin de se cacher avec le demandeur MC. Pour traiter ce problème, le serveur AS construit le MMB de façon à créer des cliques entre le demandeur et les clients de régions auparavant masquées, au lieu de chercher tous les voisins du demandeur chaque fois qu'une requête arrive.

Par conséquent, dans notre approche, le serveur AS effectue une recherche récursive les clients à partir de l'intersection de régions précédemment camouflées $(R_1 \cap R_2 \cap \cdot \cdot \cdot \cap R_{i-1})$ qui sont stockées dans le serveur AS pour reconstruire les cliques impliquant le nœud représentant la requête (l'expéditeur de la requête). En d'autres termes, le serveur AS insère chaque client des régions précédemment camouflées $(R_1 \cap R_2 \cap \cdot \cdot \cdot \cap R_{i-1})$ dans la file d'attente commune *Queue-common* qui satisfait à la condition MMB pour construire les cliques. Le détail de l'algorithme MCC est décrit dans les algorithmes 1 et 2.

Lignes 07 : Ensuite, la similarité de vitesse et la similarité de direction sont calculées. Après quoi, seul l'ensemble de camouflage répondant aux exigences de K_{global} et de la taille de la surface (A_{min}, A_{max}) est traité comme une région de camouflage qualifiée.

Lignes 08 à 11 : Par la suite, le serveur AS doit vérifier k_{global}-anonymat (définition 12). Si la condition k_{global} est remplie (candidats actifs), le serveur AS peut former un ensemble candidat de camouflage ECC_{ti} et le MBR (ECC_{ti}) peut être utilisé comme région de camouflage candidat CR_{ti}.

Lignes 13 à 14 : Après l'étape de la création de la région candidate CR_{ti}, notre algorithme passera à l'étape de la vérification des propriétés du MMB et du MAB (définition 21), pour traiter les attaques de localisation (*location attack*). Pour vérifier

les propriétés MMB et MAB, l'algorithme calcule la distance d'*Hausdorff* entre deux régions camouflées (R_{ti-1} et CR_{ti}) pour chaque client $\in EC_{ti}$, où, R_{ti-1} est une région camouflée précédemment à t_{i-1}, et CR_{ti} est une région de camouflage candidat à t_i.

Par conséquent, l'algorithme commence par la propriété MAB. Après l'obtention de l'ensemble de camouflage EC_{ti}, nous devons garantir que toutes les régions précédemment camouflées $R_{CM,ti-1}$ de tous les requêtes de l'ensemble de camouflage EC_{ti} sont couverts par le nouveau MAB de la région de camouflage candidat CR_{ti}. Pour cela, l'algorithme étend la frontière de la région CR_{ti} jusqu'au nouveau MAB couvre tous les régions précédemment camouflées $R_{CM,ti-1}$ pour chaque client MC $\in EC_{ti}$ (Lignes 01-09, Procédure de MAB (Algorithme 3)). Après la réalisation de la propriété de MAB, nous devons également vérifier la propriété de MBB. Le but des lignes 01 à 06 (fonction de MMB (Algorithme 4)) est de vérifier si la nouvelle limite de la région étendue CR_{ti} est encore couverte par le MMB des régions précédemment camouflées $R_{CM,ti-1}$ de chaque client $\in EC_{ti}$. Les propriétés de MMB et MAB (définition 21) sont des propriétés très importantes pour faire face aux attaques de localisation.

Lignes 15 à 16 : Si la propriété de MMB n'est pas remplie, donc ce processus de camouflage échoue.

Lignes 17-18 : Sinon, l'AS envoie la requête de région R_{ti} aux fournisseurs de services avec la réalisation de la propriété de *K-sharing*.

Lignes 19 : Après le succès du processus de cloaking, la région cache R_{ti} sera enregistrée dans le stock des régions camouflées.

Lignes 21-23 : Si la condition k_{global} n'est pas remplie, cet instantané est supprimé et le moteur de camouflage traite les instantanés suivants.

Algorithm 3 Procedure of MAB

Require: The candidate cloaking set ECC
Ensure: The candidate cloaked region CR
1: $CR \leftarrow MBR(ECC)$
2: **for** each query **u** in ECC **do**
3: we calculate $d = MaxMinD(R_{u,ti-1}, CR)$
4: **if** $d > (V_u * (t_i - t_{i-1}))$ **then**
5: $\delta_d \leftarrow d - V_u * (t_i - t_{i-1})$
6: CR is extended by δ_d to the direction where $R_{u,ti-1}$ is located.
7: **end if**
8: **end for**
9: Return the candidate cloaked region CR.

Algorithm 4 Function of MMB

Require: The candidate cloaked region CR and Cloaking set ECC
Ensure: The cloaked region R
1: **for** each query **u** in ECC **do**
2: **if** CR is not covered by MMB_{u,t_{i-1},t_i} **then**
3: Return **False**
4: **end if**
5: **end for**
6: **Return True**; the candidate cloaked region CR as the cloaked region R of the cloaking set EC.

5.6.5 Génération des mannequins réalistes (Dummies)

Dans les systèmes de m-business, les clients mobiles envoient des requêtes continues de leurs positions réelles. Cependant, les adversaires peuvent facilement trouver la différence entre le client réel et les mannequins dans le cas où ces mannequins sont générés aléatoirement. Par conséquent, dans notre algorithme les mannequins doivent être réels et diversifiés. En plus, ils doivent aussi satisfaire les propriétés temporelles et spatiales de la requête de client réel.

Pour cela, dans notre algorithme, le serveur AS génère les mannequins à l'intérieur du MBR de l'ensemble de camouflage EC. La requête de mannequins doit être variée et différente de celle de client mobile Q_{CM}. Le numéro d'identification des mannequins réalistes est tiré du profil factice. Nous générons des mannequins divers réalistes au lieu de supprimer la requête de client CM si k-1 autres clients mobile ne peuvent pas être trouvée, comme indiqué dans [122], [10], [11]. Pour éviter les liaisons de requêtes dans des requêtes continues, dans notre approche, nous générons des mannequins réalistes et divers afin de satisfaire les groupes d'anonymisations locales qui deviennent alors des membres de la région de camouflage.

Définition 22 (Profil Dummy)

Le profil Dummy est un fichier contenant tous les clients mobiles de notre système m-business avec les numéros d'identification des clients factices correspondants IDs, où, $N\text{-}Dummies$ représente le nombre de dummies associés à un vrai client mobile sur le profil Dummy.

Dans notre travail, nous associons pour chaque client mobile réel CM_{id} avec un ensemble de mannequins. Afin de générer un *Dummy* pour un client particulier, nous devons consulter le profil Dummy et prenons les mannequins dans un ordre topologique.

Exemple de *Profil Dummy* d'un client mobile réel : { $Id\text{-}real = C_{id1}$; $N\text{-}Dummies$ = 08 (représenter la quantité de mannequins) ; $E\text{-}Dummies$= (C_{id1}, D_1, D_2, D_3, D_4, D_5, D_6, D_7) Ensemble des mannequins}.

En plus, $Dem\text{-}Dummies$ représente le nombre de mannequins demandée pour atteindre l'exigence de la condition de Max_K ($Dem\text{-}Dummies = Max_K - |filesommets|$) (Lignes 35 à 36 de l'algorithme 1 du MCC). Si $Dem\text{-}Dummies \leq N\text{-}Dummies$, nous générons $Dem\text{-}Dummies$ mannequins tels que les mannequins $Dem\text{-}Dummies \subset$ dummy profile.

Il existe des autres travaux qui ont utilisé les mannequins comme concept pour augmenter la vie privée des systèmes basés sur l'emplacement.

Kido et al [81] ont introduit le concept de génération des localisations fictives dans LBS mais ils ont seulement considéré l'architecture du client-serveur. Dans le travail de [81], le client envoie la position réelle avec les positions fictives à la LBS. Ensuite, le LBS répond ensuite avec des réponses à la fois à la position vraie et à la position fictive. Cependant, les coûts de traitement sur l'appareil mobile pour filtrer les résultats

sont élevés. En outre, il existe un coût de communication très élevé entre le client et le LBS. Un autre inconvénient dans [81], le client peut être ré-identifié si un adversaire a une connaissance de l'histoire et en prenant l'intersection de toutes les régions avec lesquelles un adversaire est sûr que le client unique a envoyé une requête.

En outre, le travail dans [123] s'est concentré sur les systèmes basés sur le client-serveur où le serveur d'anonymisation n'est pas présent. En plus, ce travail a généré des trajectoires fictives pour éviter l'identification de trajectoires réelles. En outre, ce travail s'est concentré sur des trajectoires fictives où le serveur d'anonymisation n'est pas présent. En revanche, nous utilisons des clients mobiles factices avec diverses requêtes où le serveur d'anonymisation est présent.

5.6.5.1 Requêtes factices réalistes

Dans cette section, nous expliquerons comment générer des requêtes factices réalistes. La figure 5.8 montre un diagramme d'une requête masquée. Les coordonnées x et y représentent l'emplacement de la requête (latitude et longitude) et nous extrayons les paramètres $\triangle x$ et $\triangle y$ (tolérances spatiales) à partir de MBR ($Queue\text{-}Vertices$). Nous construisons la boîte englobante à partir de $\triangle x, \triangle y, x$ et y.

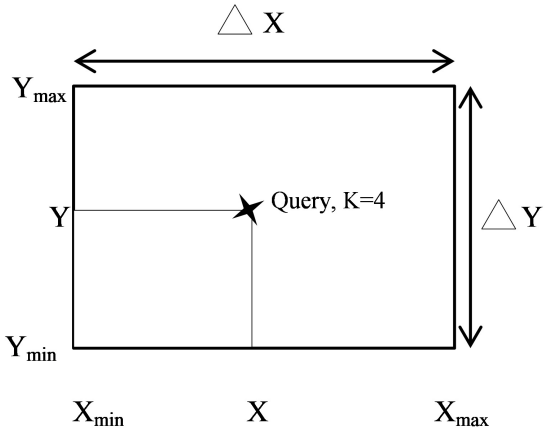


FIGURE 5.8 – Générer de requête Dummy.

Les valeurs de décalage sont calculées en fonction des propriétés spatiales de la requête (c.-à-d. x et y) comme indiqué ci-dessous :

$X_{offset} = Min(x_{max} - x, x - x_{min})/2$

$Y_{offset} = Min(y_{max} - y, y - y_{min})/2$

Par conséquent, pour chaque requête factice, nous calculons ce qui suit :

$DummyX_{offset} = x + < -1, 1 > * X_{offset}$

$DummyY_{offset} = y + < -1, 1 > * X_{offset}$

où, $DummyX_{offset}$ et $DummyY_{offset}$ sont les décalages x et y du mannequin, et <-1 ; 1> signifie un nombre aléatoire compris entre -1 et 1.

De plus, la propriété temporelle de la requête factice peut être déterminée de la même manière :

$T_{offset} = Min(T_{lt_i} - T_s, T_s - T_{lt_{i-1}})/2$

$DummyT_{offset} = T_s + < -1, 1 > *T_{offset}$

où Ts représente l'heure à laquelle la requête est créée.

De cette façon, les requêtes factices sont liées aux propriétés spatiales et temporelles de la requête réelle. Par conséquent, les adversaires peuvent être perçus les requêtes factices comme des requêtes réelles.

Dans notre travail, nous envisageons de générer des clients factices réalistes sur le serveur d'anonymisation afin de garantir l'exactitude et les résultats en temps réel du client. Nous présentons notre algorithme 5 de génération des clients factices comme suit :

Algorithm 5 Function of Realistic Dummies Generation

Require: *Id-real*, *Dem-Dummies*, Q, MBR (*Queue-Vertices*), /* Q is query*/
Ensure: the cloaked region with dummies CR, Cloaking set ECC.
1: $Workspace \leftarrow$ Extracts the minimal and maximal coordinates of the workspace (x_{min}, x_{max}) and (y_{min}, y_{max}) from MBR (*Queue-Vertices*)
2: Create Grid ((x_{min}, x_{max}), (y_{min}, y_{max}), (T_s,T_{exp})).
3: *Insert-RealClient* () // insert the real mobile client into the Grid
4: *count-Dummies* $\leftarrow$ 0 // Counter of Dummies
5: $Profile \leftarrow$ *read-dummy-profile* (*Id-real*, *N-Dummies*) //Reading the dummy profile
6: **if** *Dem-Dummies* <= *N-Dummies* **then**
7: **while** *count-Dummies* <= *Dem-Dummies* **do**
8: $t = Q_{T_s} + < -1, 1 > *T_{offset}$
9: $x = Q_x + < -1, 1 > *X_{offset}$
10: $y = Q_y + < -1, 1 > *Y_{offset}$
11: $id \leftarrow profile.nextID()$
12: $Q' = Diversify(Q)$ // diversifying the dummy query
13: $newDummy \leftarrow createDummy(id, x, y, t, Q')$
14: $dummyMap.put(newDummy)$
15: $Queue\text{-}Vertices \leftarrow newDummy$
16: *count-Dummies* + +
17: **end while**
18: $ECC \leftarrow Queue\text{-}Vertices$ with the Dummies
19: $CR \leftarrow MBR(ECC)$
20: return True
21: **else**
22: Insert Q_{MC} in the *Pre-cloaked* Pre_clk
23: return False // No Dummies
24: **end if**

Cette méthode garantit que le point de requête du client mobile réel n'est pas le même que le point de requête des mannequins au lieu d'utiliser un bâtiment différent ou une adresse symbolique dans la région MBR.

Dans **la ligne 05**, nous lisons le profil Dummy du client mobile, de sorte que l'identification du client mobile, le nombre total de mannequins requis, la requête du client réel, le MBR de $Queue\text{-}Vertices$ et les coordonnées du client réel sont passés comme paramètres.

Dans **la ligne 11**, à partir du profil Dummy, nous générons toutes les identifications factices.

Dans **la ligne 07-17**, nous sommes assurés que les propriétés temporelles et spatiales des mannequins sont liées à un client mobile.

En **ligne 12**, pour éviter l'attaque de l'homogénéité, nous diversifions la requête. Ensuite, à **la ligne 13**, nous créons le nouveau mannequin et le stockons en mémoire.

5.7 Analyse de sécurité

Lorsque les informations telles que la localisation du client, la connaissance de certains contenus de requête et l'échantillon d'un ensemble de camouflage de certains instantanés sont facilement accessibles par un tiers, plusieurs types d'attaques peuvent se produire tels que les attaques de localisation, query tracking attack [1] et query homogeneity attacks [13].

Cette section montre comment nous traitons chaque type d'attaque. Nous procédons comme suit :

- ✓ **Attaque de localisation :** pour surmonter cette attaque, nous devons nous assurer des propriétés de MMB et MAB (Définition 21).
- ✓ **Tracking and Linking Attack :** Un adversaire peut lancer une attaque par suivi de requête en calculant $R_{t_i} \cap R_{t_{i+1}}$ lorsqu'il obtient les régions camouflées du client CM en t_i et t_{i+1}. Nous utilisons l'exigence k_{global} (Définition 12) pour surmonter les attaques de suivi de requêtes et les attaques de liaison. La réalisation de la propriété *k-sharing* (Définition 09) est très importante pour surmonter les attaques d'échantillonnage de requête.

  Par conséquent, les clients de l'ensemble de camouflage doivent être sous la forme de la clique (définition 07) et devraient avoir des mouvements semblables (définition 13) au demandeur mobile pour surmonter les attaques de liaison de requête et les attaques d'échantillonnage de requête.
- ✓ **Homogeneity Attack :** Si tous les clients de la région camouflée ont demandé le même service, nous devons assurer la propriété de *L-diversit* pour faire face à l'attaque d'homogénéité.

5.8 Conclusion

Dans ce chapitre, nous avons présenté nos contributions et l'architecture générale de notre approche. En plus, une nouvelle l'algorithme de protection de la vie privée de client mobile basé clique est proposée en tenant compte des mouvements des clients mobiles comme les caractéristiques de vitesse, accélération et direction. Les résultats d'analyse montrent que l'algorithme peut obtenir un bon équilibre entre QoS et la vie privée.

Dans le chapitre suivant nous allons appliquer nos propositions, puis étudier les résultats expérimentaux.

Chapitre 6

Expérimentation et évaluation

6.1 Introduction

Dans le but de réaliser et valider les idées proposées dans le chapitre précédent, le présent chapitre montre les outils et les configurations utilisées afin de développer notre système. Dans ce chapitre, nous présentons une mise en œuvre de nos contributions citées précédemment, afin de juger nos propositions et d'évaluer l'efficacité de notre approche de sécurité. Puis, nous présentons une discussion sur les résultats pour chaque évaluation.

6.2 Environnement Technologique

Dans cette section, nous allons présenter les plateformes utilisées afin de réaliser notre système. L'approche proposée dans notre travail est implémentée sur un ordinateur de processeur Core I3 avec une RAM de 16 Go sous Windows 8.

6.2.1 Langage java et IDE

Nous avons utilisé le langage JAVA afin de démontrer la faisabilité de notre contribution. JAVA développé dans les laboratoires de SUN Microsystems, présente plusieurs avantages. En termes de l'environnement de développement, nous avons utilisé Netbeans.

NetBeans est un projet open source ayant un succès et une base d'utilisateur très large, une communauté en croisance constante, et près 100 partenaires mondiaux et des centaines de milliers d'utilisateur à travers le monde. Sun Microsystems a fondé le projet open source NetBeans en Juin 2000 et continue d'être le sponsor principal du projet.

L'EDI NetBeans est un environnement de développement - un outil pour les programmeurs pour écrire, compiler, déboguer et déployer des programmes. Il est écrit en Java - mais peut supporter n'importe quel langage de programmation. Il y a également

un grand nombre de modules pour étendre l'EDI NetBeans. L'EDI NetBeans est un produit gratuit, sans aucune restriction quant à son usage [139].

6.2.2 Générateur d'objets mobile

Nous avons utilisé le générateur Thomas Brinkhoff Générateur afin de générer les mouvements des clients de notre système.

6.2.2.1 Jeux de données (Data Set)

afin de tester l'efficacité de notre approche, nous avons utilisé le générateur de Brinkhoff [3] pour générer des traces de clients mobiles sur le réseau réel de la route des villes de Oldenburg en Allemagne.

6.2.2.2 Thomas Brinkhoff Générateur

Ce générateur combine un réseau réel avec les propriétés définies par l'utilisateur de l'ensemble de données résultant. En plus, il est basé sur l'observation que les objets se déplacent souvent selon un réseau. Cette observation est valable, par exemple, pour le trafic routier ainsi que pour le trafic ferroviaire. La figure 6.1 illustre l'interface graphique du générateur.

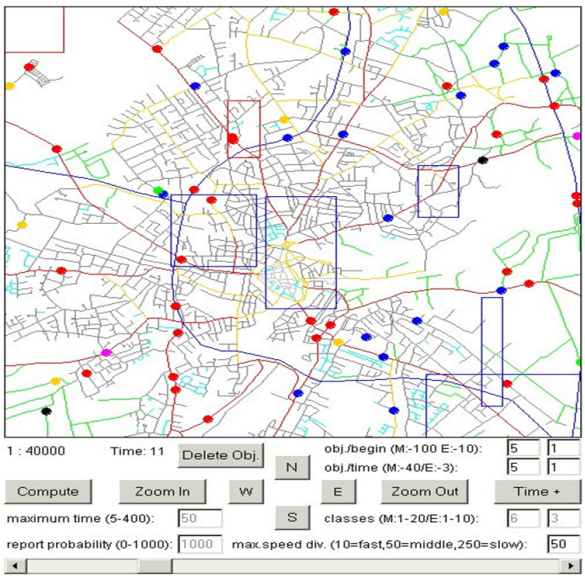


FIGURE 6.1 – Visualisation du générateur de Brinkhoff [3].

Le générateur utilise un modèle temporel discret : la période entière est divisée par n horodatage (timestamps). À chaque timestamps, de nouveaux objets en mouvement sont générés et les objets existants sont déplacés ou supprimés car ils ont atteint leur destination. Chaque objet en mouvement appartient à une classe qui spécifie le comportement de l'objet. Par exemple, la vitesse (maximale) est définie par une telle classe. Chaque bord du réseau appartient à une classe de bord, qui définit la limite de vitesse

et la capacité d'un bord. Si le nombre d'objets traversant un bord à un horodatage dépasse la capacité spécifiée, la limite de vitesse sur ce bord sera réduite. De plus, des objets dits externes peuvent être générés afin de simuler l'impact des conditions météorologiques ou des influences similaires.

Il existe des objets externes, qui sont présents sur toute la période, et d'autres, qui sont créés au cours de la simulation et sont supprimés plus tard. Les objets externes peuvent changer leur position et leur forme (rectangulaire) au fil du temps. Si un objet en mouvement se trouve dans la zone d'un objet externe, sa vitesse est influencée selon les paramètres de la classe à laquelle l'objet externe appartient. Le générateur de Brinkhoff est écrit en Java 1.1.

Une interface graphique permet de définir les paramètres et de visualiser le réseau et les objets générés (La figure 6.1).

Le réseau utilisé par le générateur est spécifié par des fichiers texte simples. La même chose vaut pour la sortie : les objets signalés sont écrits dans un fichier texte ou dans une base de données. L'exemple suivant montre une partie sélectionnée de ce fichier de sortie ; chaque ligne comprend le type d'événement, l'ID d'objet, la classe de l'objet mobile, l'index de l'horodatage et les coordonnées x, y comme. La figure 6.2 illustre une partie de ce fichier.

Type d'événement	ID d'objet	Classe	Time stamp	X	Y
newpoint	0	3	0	20435	19558
point	0	3	1	20455	19688
newpoint	5	0	1	13858	10979
point	0	3	2	20475	19818
point	5	0	2	13800	11627
newpoint	10	1	2	5079	18012
point	0	3	3	20496	19948
point	5	0	3	13504	12223
point	10	1	3	5334	17822
newpoint	15	0	3	13566	20167
disappearpoint	0	3	4	20493	20078
point	5	0	4	13258	12841
point	10	1	4	5981	17832
point	15	0	4	13612	19876

FIGURE 6.2 – Exemple montre une partie sélectionnée de fichier de sortie [3].

6.3 Implémentation et Évaluation

Dans cette section, nous évaluons l'efficacité de l'approche que nous proposons en effectuant un ensemble d'expériences. Pour évaluer, nous avons utilisé les métriques suivantes : garantie de la vie privée, la qualité de service et performances. À notre connaissance, en raison des problèmes d'intérêt commercial et de protection de la vie privée, il n'y a pas vraiment d'ensemble de données à grande échelle sur les objets en mouvement publié. Comme de nombreux ouvrages, nous utilisons le célèbre générateur

d'objets mobiles Thomas Brinkhoff [3] sur la carte routière d'Oldenburg pour générer les objets mobiles dans le système comme le montre la figure 6.3.

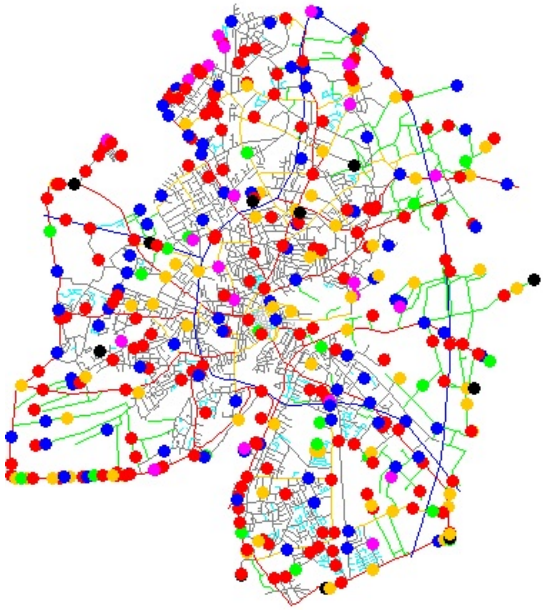


FIGURE 6.3 – Utilisateurs générés sur la carte routière d'Oldenbourg.

Dans les paramètres par défaut, 2000 clients mobiles sont générés se déplaçant le long de la carte avec des vitesses variées pour 100. L'intervalle de requête est fixé à 20 s. Par conséquent, à partir de ce générateur, nous pouvons obtenir les vitesses et les emplacements correspondants de tous les clients. Par défaut, chaque requête définit : le paramètre de l-Diversity (l est un nombre aléatoire entre [0, 3]) ; et le niveau de vie privée k avec un nombre aléatoire entre [2, 4]. Nous avons comparé notre algorithme avec les autres algorithmes nommés V-DCA [11], D-TC [140] et GCA [141]. Nous avons implémenté nos algorithmes de camouflage avec Java. Le tableau 6.1 présente les paramètres par défaut du système utilisés dans notre expérience.

6.3.1 Critères et paramètres d'évaluation

Tout d'abord pour analyser en détail nos résultats d'expérimentations et mesurer les performances de notre approche, nous définissons d'abord quelques paramètres. Nous évaluons nos algorithmes sous trois aspects : garantie de la vie privée, qualité de service et la performance :

6.3.1.1 Garantie de la vie privée :

La garantie de vie privée représentée par le KPercentage. Pour une requête continue, les clients masqués dans t=0 (R_0) doivent être dans les snapshots suivants autant que

possible.

$$K_{Percentage} = (|R_0 \cap R_1 \cap R_2 \cap ... \cap R_n|/|R_0|) * 100 \tag{6.1}$$

où **n** est le nombre maximum d'ensembles camouflés qui répondent aux exigences de vie privée et de qualité dans les instantanés continus. La valeur maximale de k est $|R_0|$, donc un K plus grand signifie une meilleure protection de la vie privée pour un algorithme particulier. Par conséquent, les paramètres $< K, n >$ peuvent être utilisés pour mesurer la performance des algorithmes de cloaking.

6.3.1.2 Qualité de service QoS :

Puisque les clients de m-business restant éloignés peuvent réduire l'exactitude des résultats et en plus les réponses de requête sont plus précises dans une plus petite région masquée, nous évaluons les *Qos* en utilisant deux paramètres : la zone de camouflage moyenne et la distance moyenne pendant la durée de vie de la requête. Par conséquent, une valeur plus petite pour les deux métriques indique une meilleure qualité de service.

✓ ***Distance moyenne :*** La distance moyenne DistanceAvrg $(q; R_i)$ est calculée comme suit :

$$Distance_{Avrg}(q, R_i) = \sum_{i=1to(k-1)} Distance(q, q'_i)/k - 1 \tag{6.2}$$

où, au moment de l'instantané **i**, R_i est une région masquée du client de la requête q, et $Distance(q, q')$ est la distance entre le client de la requête q et le client q' qui a été masqué avec q dans R_i. Par conséquent, la valeur moyenne de la distance entre le client de la requête q et les clients masqués ensemble représente la distance moyenne.

Pour une requête continue avec n snapshots, la distance moyenne $Distance_{Avrg}(q)$ de tous les snapshots est :

$$Distance_{Avrg}(q) = \sum_{i=1ton} Distance_{Avrg}(q, R_i)/n \tag{6.3}$$

✓ ***Zone de camouflage moyenne :*** est la moyenne de la superficie totale de toutes les régions de camouflage réussies dans la période active d'une requête, la zone de camouflage moyenne $Area_{Avrg}(q)$ est calculée comme suit :

$$Area_{Avrg}(q) = \sum_{i=1ton} Area(R_i)/n \tag{6.4}$$

TABLE 6.1 – Paramètres d'expérience.

Paramètres	Paramètres par défaut
Nombre de profil des clients	2000
Nombre de snapshots	1-100
Vitesse	Vitesses variées
k (Privacy Level)	Choisi au hasard parmi [2-10]
Catégorie de requête (l-Diversity)	Choisi au hasard parmi [0-3]
Intervalle de requête	20s

6.3.1.3 Performance :

La performance est la capacité de l'algorithme à trouver les clients les plus proches du client de la requête q (le demandeur) ; en d'autres termes, il représente le temps nécessaire pour trouver la région de camouflage. Nous évaluons la performance en utilisant le temps moyen de cloaking comme suit :

$$CloakingTime_{Avrg} = \sum_{i=1ton} C_{time}(R_i)/n \tag{6.5}$$

$C_{time}(Ri)$ représente le temps de cloaking pour chaque région camouflée et **n** représente le nombre d'instantanés de la requête q. Pour obtenir un mécanisme de protection de la vie privée efficace, le temps de cloaking doit être suffisamment court.

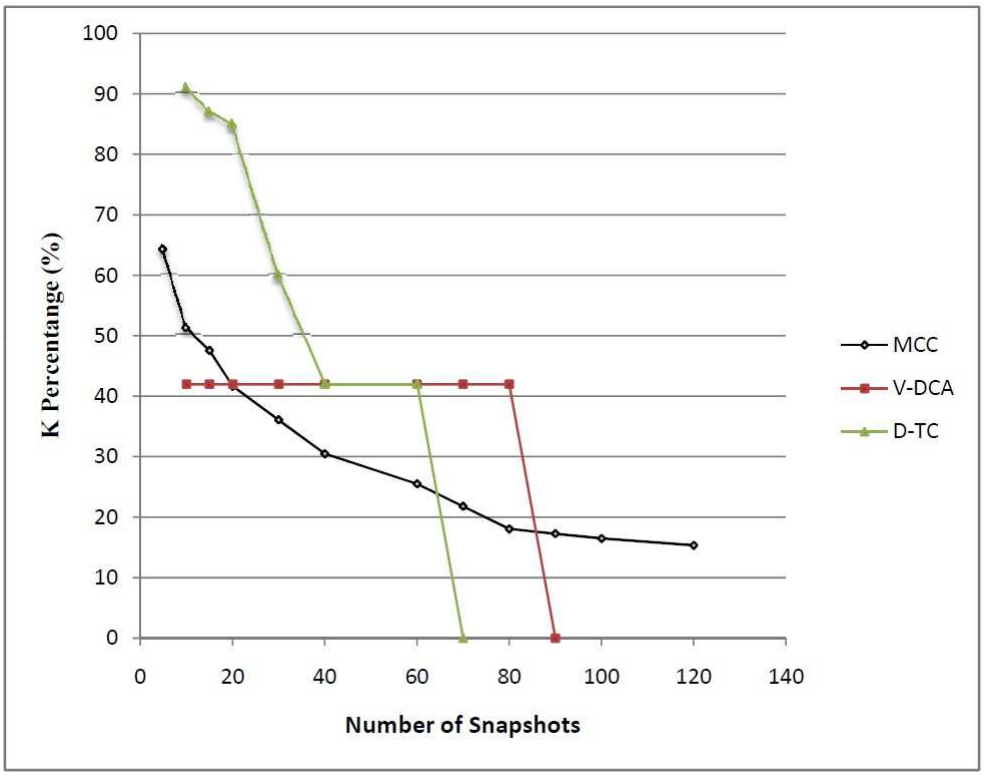


FIGURE 6.4 – Évaluation de la garantie de la vie privée.

6.4 Résultats d'évaluation

Les paramètres k et n peuvent être utilisés pour mesurer les performances des algorithmes de Cloaking. Un algorithme de cloaking est censé protéger efficacement contre les attaques par suivi des requêtes s'il maintient autant de clients que possibles de R_0. La figure 6.4 montre les résultats de la comparaison des garanties de vie privée. Comme le montre la figure 6.4, le **n** influence le pourcentage d'intersection ($K_{percentage}$) de l'instantané consécutif masqué avec succès. Parmi les autres algorithmes, nous pouvons trouver que le $K_{percentage}$ de notre algorithme **MCC** est le plus élevé.

En comparaison avec **D-TC** et **V-DCA**, le **MCC** a un $K_{percentage}$ relativement plus grand lorsque le nombre de snapshots atteint 90 snapshots pour **V-DCA** et 70 snapshots pour **D-TC** ; en outre, le $K_{percentage}$ du **MCC** est beaucoup plus stable, avec un 0,15 pour plus de 120 instantanés, comme le montre la figure 6.4. En comparaison avec **D-TC** et **V-DCA**, les résultats suggèrent que notre algorithme **MCC** garde plus de clients de la première région camouflée (R_0) dans les instantanés consécutifs.

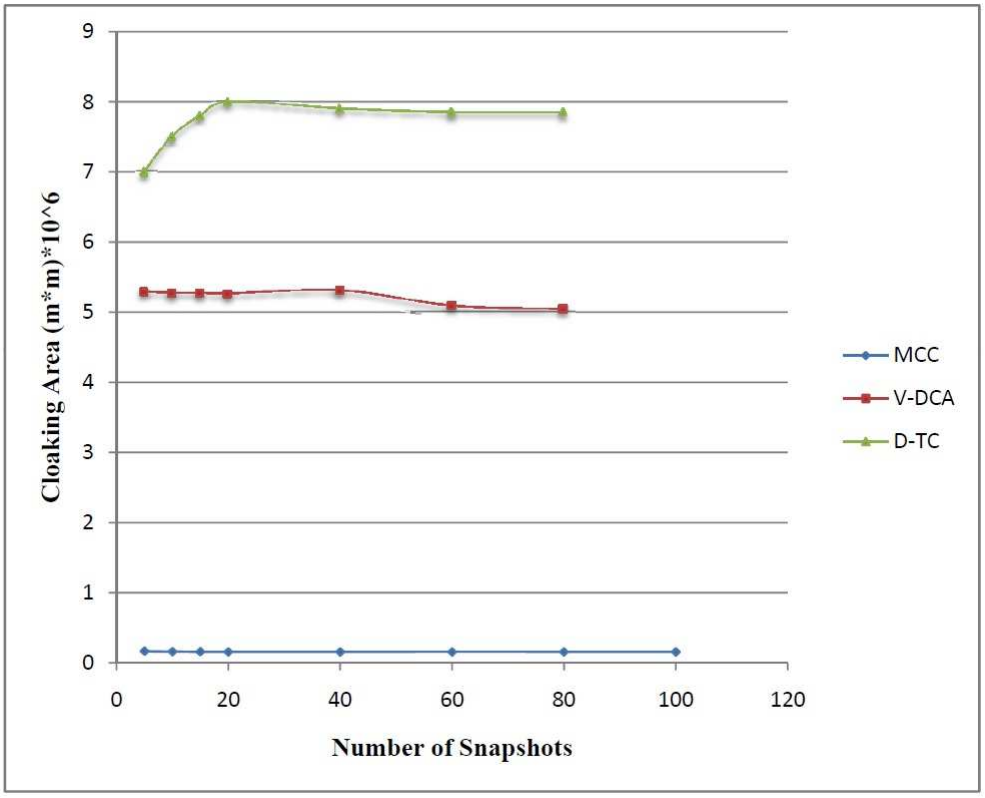


FIGURE 6.5 – Évaluation de la qualité de service (cloking Area).

Les expériences de la figure 6.4 montrent que les performances du **MCC** sont bien meilleures avec les critères d'évaluation **n** et $K_{percentage}$ (définition 23). En effet, dans notre approche, nous tenons compte des propriétés du MMB et du MAB (définition 20), ainsi que de la similitude de la vitesse et de la direction. Nous utilisons les paramètres

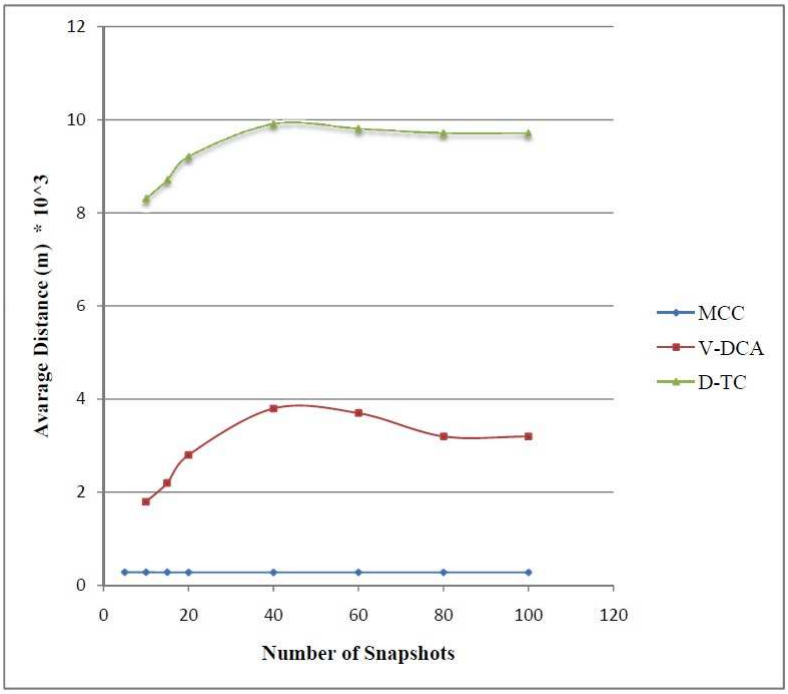


FIGURE 6.6 – Évaluation de la qualité de service(Average Distance).

mentionnés ci-dessus (zone de camouflage moyenne et distance moyenne) pendant la durée de vie de la requête, pour faire la comparaison des Qos des trois algorithmes (**MCC**, **V-DCA** et **D-TC**) ; la figure 6.5 et la figure 6.6 montrent les résultats de la comparaison.

En comparaison avec D-TC et V-DCA, la zone de camouflage moyenne et la distance moyenne du MCC sont beaucoup plus petites et plus stables que les autres, ce qui montre que le MCC peut fournir un Qos plus stable et plus élevé que les autres algorithmes, comme le montrent la figure 6.5 et la figure 6.6. **D-TC** et **V-DCA** peuvent préserver la garantie de vie privée, mais conduisant à la diminution de la qualité de service. La figure 6.7 illustre la performance des algorithmes en termes de temps de cloaking.

Dans les premiers instantanés, le **MCC** fonctionne mieux que **GCA**. En comparant avec **D-TC** et **V-DCA**, comme le montre la figure 6.7, **V-DCA** et **D-TC** fonctionnent mieux que **MCC**. En effet, dans notre approche, nous considérons beaucoup plus de facteurs pour une meilleure protection de la vie privée, tels que la construction de cliques, la similarité de la vitesse et la similarité de la direction, en plus le processus de découverte des cliques prend du temps.

Toutefois, selon les résultats de l'évaluation et la comparaison des algorithmes, le **MCC** peut offrir un bon équilibre entre qualité de service, performances et la protection de la vie privée. Les expériences montrent que nos algorithmes proposés peuvent assurer une meilleure protection de la vie privée que le **D-TC** et le **V-DCA** lorsqu'ils

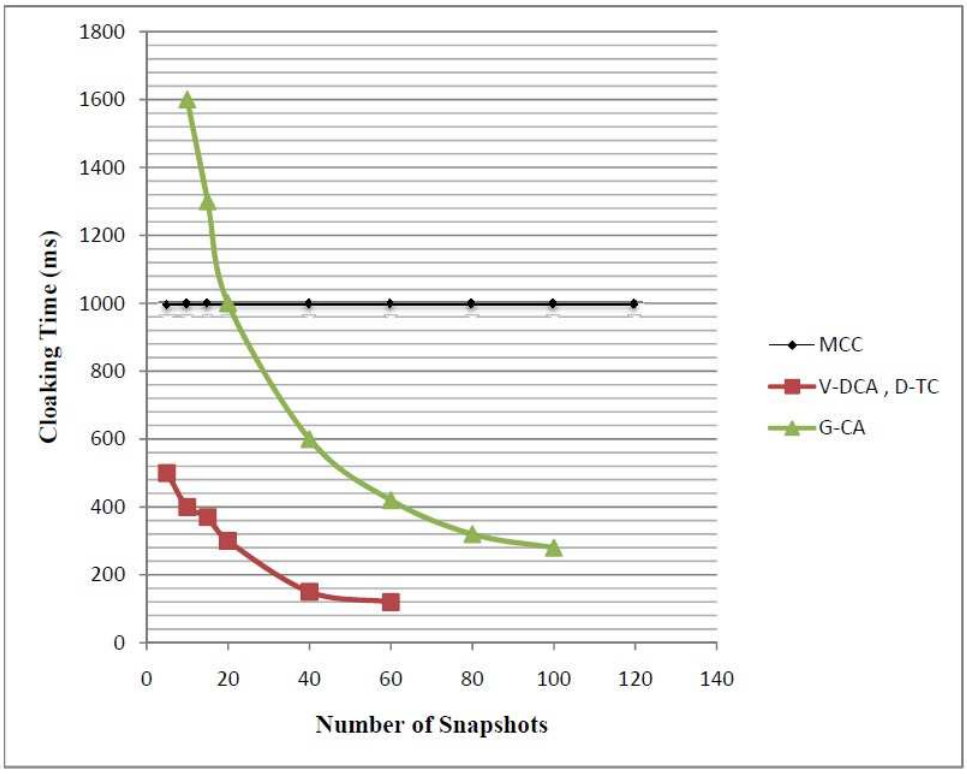


FIGURE 6.7 – Évaluation des performances.

fournissent la même qualité de service aux requêtes continues.

6.5 Conclusion

Au cours de ce chapitre, nous avons présenté les outils et les plateformes utilisées afin d'implémenter notre approche de sécurité. Après, nous avons exposé quelques formes graphiques pour montrer l'efficacité de notre approche suivie par des discussions sur les résultats collectés.

Chapitre 7

Conclusion Générale et Perspectives

7.1 Conclusion Générale

La prolifération des appareils mobiles compatibles avec la localisation entre les mains des utilisateurs a entraîné un développement rapide de m-business. Bien que le m-business puisse offrir des possibilités attrayantes et bénéfiques aux utilisateurs, il pose des risques importants pour la vie privée de l'utilisateur. En raison de la nature sensible des informations de localisation, ces risques peuvent se traduire par un préjudice matériel, moral et même physique important. En plus, la collecte, l'utilisation et la divulgation d'informations de localisation personnelles via ces services soulèvent de graves problèmes de vie privée, notamment en raison de la nature sensible des informations de localisation.

Avec des fournisseurs de services non fiables, un adversaire peut accéder à des informations sensibles sur des personnes en fonction des requêtes basées sur la localisation qu'ils ont émises. Dans de nombreux scénarios de la vie réelle, les dispositifs mobiles ont été utilisés pour traquer des emplacements personnels. Pour faire face aux menaces de la vie privée dans le m-business, plusieurs approches de cloaking spatial ont été proposées pour préserver la vie privée des utilisateurs. Les exigences de la vie privée peuvent être représentées en termes de k-anonymat (c.-à-d., qu'il est impossible de distinguer un emplacement d'utilisateur parmi k utilisateurs) et/ou zone spatiale minimale (c.-à-d., un emplacement d'utilisateur est caché dans une région avec un seuil de taille minimum)

Ainsi, sans préserver la vie privée de l'utilisateur et avec la possibilité de collecter et enregistrer les données de localisation précises de l'utilisateur par les fournisseurs non fiables, dans ce cas la vie privée l'utilisateur mobile peuvent être divulguées aux des tierces parties. Par conséquent, la vie privée de l'utilisateur est un problème fondamental pour le déploiement de m-business.

Dans cette thèse, nous proposons une approche de protection de la vie privée de l'utilisateur dans le M-business [131]. Comme nous avons mentionné, précédemment, la

plupart des approches de cloaking existants ne concernent que les requêtes instantanées (Snapshot) de l'utilisateur. Ainsi, notre approche de cloaking concerne la protection de la vie privée pour les requêtes continues (Continuous). Pour résoudre ce problème, nous avons utilisé un modèle de graphe pour formaliser le problème et l'avons transformé en un problème de recherche de cliques de K nœuds dans le graphe.

En plus, la plupart des approches de cloaking existants ne peuvent pas efficacement se défendre contre une série d'attaques dans le même processus de cloaking car ils ne concernent qu'un seul type d'attaque dans le processus de cloaking. En outre, notre approche prend en compte la similarité de vitesse et de direction des utilisateurs pour s'assurer que les utilisateurs masquées au temps t_i ont une plus grande probabilité de rester ensemble au temps t_{i+1}. Autrement dit, les utilisateurs qui sont camouflés ensemble doivent être relativement proches de la distance pour avoir la région de cloaking relativement petite et par conséquent une bonne QoS. En plus, nous avons combiné les paramètres A_{min} et A_{max} avec k_{local} et k_{global} pour équilibrer la vie privée et la Qos. Contrairement aux travaux précédents, dans notre travail, nous avons abordé la protection de la vie privée de l'emplacement et la vie privée des requêtes de l'utilisateur en même processus de protection.

Dans cette thèse, nous avons fait, en premier temps, un survol sur l'état de l'art qui consiste à présenter les définitions de la technologie mobile, le m-business, la protection de la vie privée et nous avons aussi discuté les mécanismes de protection. Afin de montrer l'intérêt de notre travail, dans le quatrième chapitre, nous avons donné une présentation avec une synthèse sur les travaux réalisés pour la résolution du problème de protection de la vie privée. Afin de résoudre le problème posé, le cinquième chapitre comporte notre approche proposé qui est basée sur cloaking spatiale.

Afin de valider l'approche utilisée, dans le sixième chapitre, nous avons montré les outils utilisés pour arriver à des résultats. En outre, nous avons défini les paramètres utilisés pour ajuster les algorithmes utilisés dans l'approche. Pour finaliser la mise en œuvre, nous avons introduit une discussion sur les résultats obtenus afin d'analyser les résultats collectés.

7.2 Perspectives

Dans le futur et comme perspectives de ce travail, nous pensons à introduire des points comme extensions de notre travail futur ou pour les chercheurs dans ce domaine. Nous suggérons les problèmes suivants :

- ✓ Attaque d'apprentissage profond (Machine/deep learning attack) : L'intégration d'algorithmes d'apprentissage et d'autres méthodes d'apprentissage en profondeur pose un énorme défi à la vie privée de l'emplacement, ainsi que la quantité massive de données en ligne. Par exemple, les méthodes actuelles d'apprentissage

en profondeur peuvent faire des prédictions sur les géolocalisations basées sur les photos personnelles de réseaux sociaux et effectuer des types de détection d'objets en fonction de leur capacité à analyser des millions de photos et de vidéos.

- ✓ Environnements de réseaux routiers : Les techniques de protection de la vie privée d'emplacement existantes considèrent principalement l'espace euclidien où les utilisateurs peuvent se déplacer librement. En réalité, la majeure partie du mouvement de l'objet est limitée par le réseau routier. Il n'est pas pratique d'appliquer directement les techniques de protection de la vie privée de l'emplacement existant à l'environnement du réseau routier, car les adversaires auraient plus d'information sur les emplacements possibles des utilisateurs, dérivées de la connaissance du réseau routier. Il est donc important de concevoir de nouvelles techniques spécialisées d'anonymisation des emplacements et de traitement des requêtes pour préserver la vie privée dans les environnements de réseaux routiers.
- ✓ Perspectives des utilisateurs : Les infrastructures existantes qui protègent la vie privée sont conçus à partir des technologies prospectives. Il est encore nécessaire d'étudier le problème de vie privée de l'emplacement du point de vue de l'utilisateur. Par exemple, comment un utilisateur occasionnel peut-il définir les exigences de vie privée ? Est-il possible de définir les niveaux de la vie privée comme bas, moyen et strict, puis les utilisateurs choisiraient parmi eux ? Comment un utilisateur peut-il faire un compromis entre les exigences de protection de la vie privée et la qualité des services ? Comment l'utilisateur peut-il évaluer le risque de la vie privée pour l'utilisation d'un certain service ?

Annexe A

Liste des publications

A.1 Revues Internationales

Ahmed Aloui, Okba Kazar. "Mobile business approach based on mobile agent", International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3), ISSN 2225-658X : 682-692, 2012.

Ahmed Aloui, Okba Kazar and Omary Fouziya. "An Efficient Approach for Privacy-Preserving of the Client's Location and Query in M-Business Supplying LBS Services". International Journal of Wireless Information Networks, 1-22, **Springer**, **2020**. **(Disponible enligne)**.

A.2 Conférences Internationales

Ahmed Aloui, Okba Kazar and Saber Benharzallah : «A mobile agent for M-Business approach» ; 5th. International Conference on Information Systems and Economic Intelligence (SIIE2012) in Djerba – Tunisie. pp.136-143. ISBN 9978-9973868-19-0.

Ahmed Aloui, Okba Kazar et ZERDOUMI Oussama. "Architecture for mobile business based on mobile agent". In : 2012 International Conference on Multimedia Computing and Systems. IEEE, 2012. p. 954-958 (ICMCS'12) in Tangier, Morocco.

Ahmed Aloui, Okba Kazar and BOUREKKACHE Samir, "Security study of m-business : Review and important solutions". In : 2015 6th International Conference on Information Systems and Economic Intelligence (SIIE). IEEE, 2015, In Tunisia p. 90-96.

A.3 Conférences Nationales

Ahmed Aloui and Okba Kazar, "Location privacy in m-business", International Workshop on Artificial Intelligence and Information Communication Technologies (IWAIICT'15), 23-24 Novembre 2015, Biskra- Algérie.

Bibliographie

[1] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in *International Symposium on Spatial and Temporal Databases*, pp. 258–275, Springer, 2007.

[2] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Personal and ubiquitous computing*, vol. 18, no. 1, pp. 163–175, 2014.

[3] T. Brinkhoff, "A framework for generating network-based moving objects," *GeoInformatica*, vol. 6, no. 2, pp. 153–180, 2002.

[4] Y. Tan, "Research on scheme and technology for mobile user's trajectory privacy protection," in *IOP Conference Series : Earth and Environmental Science*, vol. 234, p. 012116, IOP Publishing, 2019.

[5] A. Malm, "Mobile location-based services - 9th edition," tech. rep., Berg Insight, August 2015.

[6] M. Mohammadian, D. Hatzinakos, P. Spachos, and R. Jentzsh, "An intelligent and secure framework for wireless information technology in healthcare for user and data classification in hospitals," in *Handbook of Research on Advancing Health Education through Technology*, pp. 452–479, IGI Global, 2016.

[7] C.-Y. Chow, M. F. Mokbel, and X. Liu, "Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments," *GeoInformatica*, vol. 15, no. 2, pp. 351–380, 2011.

[8] L. Gonzalez, P. Wightman Rojas, M. Labrador, *et al.*, "A survey on privacy in location-based services," *Ingeniería y Desarrollo*, vol. 32, no. 2, pp. 314–343, 2014.

[9] B. Gedik and L. Liu, "Location privacy in mobile systems : A personalized anonymization model," in *Distributed computing systems, 2005. ICDCS 2005. Proceedings. 25th IEEE international conference on*, pp. 620–629, IEEE, 2005.

[10] X. Pan, J. Xu, and X. Meng, "Protecting location privacy against location-dependent attacks in mobile services," *IEEE Transactions on Knowledge and Data Engineering*, vol. 24, no. 8, pp. 1506–1519, 2012.

[11] Y. Wang, L.-p. He, J. Peng, T.-t. Zhang, and H.-z. Li, "Privacy preserving for continuous query in location based services," in *Parallel and Distributed Systems*

(ICPADS), 2012 IEEE 18th International Conference on, pp. 213–220, IEEE, 2012.

[12] L. Stenneth, S. Y. Phillip, and O. Wolfson, "Mobile systems location privacy :"mobipriv" a robust k anonymous system," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on*, pp. 54–63, IEEE, 2010.

[13] F. Liu, K. A. Hua, and Y. Cai, "Query l-diversity in location-based services," in *Mobile Data Management : Systems, Services and Middleware, 2009. MDM'09. Tenth International Conference on*, pp. 436–442, IEEE, 2009.

[14] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacygrid," in *Proceedings of the 17th international conference on World Wide Web*, pp. 237–246, ACM, 2008.

[15] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper : Query processing for location services without compromising privacy," in *Proceedings of the 32nd international conference on Very large data bases*, pp. 763–774, VLDB Endowment, 2006.

[16] K. Stanoevska-Slabeva, "The transition from e-to m-business chances and challenges for enterprises," *BLED 2004 Proceedings*, p. 48, 2004.

[17] A. Tsalgatidou and E. Pitoura, "Business models and transactions in mobile electronic commerce : requirements and properties," *Computer Networks*, vol. 37, no. 2, pp. 221–236, 2001.

[18] S. Liao, Y. P. Shao, H. Wang, and A. Chen, "The adoption of virtual banking : an empirical study," *International journal of information management*, vol. 19, no. 1, pp. 63–74, 1999.

[19] I. Clarke III, "Emerging value propositions for m-commerce.," *Journal of Business Strategies*, vol. 25, no. 2, 2008.

[20] V. Terziyan, "Ontological modelling of e-services to ensure appropriate mobile transactions," *Intelligent Systems in Accounting, Finance & Management*, vol. 11, no. 3, pp. 159–172, 2002.

[21] R. Kalakota, M. Robinson, and D. R. Kalakota, *M-business : The race to mobility*. McGraw-Hill New York, NY, 2002.

[22] L. Kenneth and A. John, "Improving returns on m-commerce investments," *Journal of Business Strategy*, vol. 22, no. 5, pp. 12–16, 2001.

[23] T. O'Driscoll, D. Reibstein, and V. Shankar, "Mobile e-business : disruptive technology or untethered extension of business as usual ?," *University of Maryland*, 2002.

[24] S. Dittel, "Future worldwide trends in m-business." http://www.iwi.unihannover.de/lv/seminar_ss03/Dittel/htm%20Seiten/Home.htm. Erişişm tarihi 16.02.2012.

[25] H.-G. Kemper and E. Wolf, "Iterative process models for mobile application systems : A framework," *ICIS 2002 Proceedings*, p. 37, 2002.

[26] F. Lehner, "Mobile knowledge management," in *Geschäftsprozesse mit Mobile Computing*, pp. 153–172, Springer, 2002.

[27] G. Shih and S. S. Shim, "A service management framework for m-commerce applications," *Mobile Networks and applications*, vol. 7, no. 3, pp. 199–212, 2002.

[28] J. Zhang and Y. Yuan, "M-commerce versus internet-based e-commerce : the key differences," *AMCIS 2002 Proceedings*, p. 261, 2002.

[29] I. Clarke III, "Emerging value propositions for m-commerce," *Journal of business strategies*, vol. 18, no. 2, p. 133, 2001.

[30] H.-S. Tsai and R. Gururajan, "Mobile business : an exploratory study to define a framework for the transformation process," *Collaborative Decision Making In The Internet Era*, pp. 1–11, 2005.

[31] B. Chirantan, "The Operational Differences Between E-Business & M-Business." http://smallbusiness.chron.com/operational-differences-between-ebusiness-mbusiness-25054.html. Accessed 01 October 2019.

[32] R. Bonnici, "The 2012 Channel Marketing Preference Survey," tech. rep., 2013.

[33] R. Bonnici, "The Digital Marketing Cafe," tech. rep., 2013.

[34] M. Glatin, *La geolocalisation nouvelle arme des marketeurs*. Bluffy : Ed. Kawa, 2014.

[35] N. Chan and H. Lars, "Introduction to location-based services," *Lund University GIS Centre*, 2003.

[36] X. Pan, W. Chen, L. Wu, C. Piao, and Z. Hu, "Protecting personalized privacy against sensitivity homogeneity attacks over road networks in mobile services," *Frontiers of Computer Science*, vol. 10, no. 2, pp. 370–386, 2016.

[37] C. Piao, X. Li, X. Pan, and C. Zhang, "User privacy protection for a mobile commerce alliance," *Electronic Commerce Research and Applications*, vol. 18, pp. 58–70, 2016.

[38] T. Scassa and A. Sattler, "Location-based services and privacy," *Canadian Journal of Law and Technology*, vol. 9, no. 1 & 2, 2011.

[39] D. Keely, "A security strategy for mobile e-business," *NewYork : IBM*, 2001.

[40] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, vol. 25, no. 1, p. 166, 1968.

[41] C. C. Portal, "Common Criteria Portal"," 2017.

[42] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization : Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.

[43] D. J. Solove, "I've got nothing to hide and other misunderstandings of privacy," *San Diego L. Rev.*, vol. 44, p. 745, 2007.

[44] C. E. Tucker, "Social networks, personalized advertising, and privacy controls," *Journal of marketing research*, vol. 51, no. 5, pp. 546–562, 2014.

[45] L. Sweeney, "k-anonymity : A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[46] E. Turban, D. King, J. K. Lee, T.-P. Liang, and D. C. Turban, "E-commerce : Regulatory, ethical, and social environments," in *Electronic Commerce*, pp. 689–730, Springer, 2015.

[47] C. Arthur, "iPhone 4 keeps record of everywhere you go"," 2011.

[48] L. Liu and M. T. Özsu, *Encyclopedia of database systems*, vol. 6. Springer New York, NY, USA :, 2009.

[49] E. Tanin, R. Zhang, and L. Kulik, "Spatio-temporal database research at the university of melbourne," *ACM SIGMOD Record*, vol. 38, no. 3, pp. 35–39, 2010.

[50] J. Harper, "The digital person : Technology and privacy in the information age," *Cato Journal*, vol. 25, no. 3, p. 642, 2005.

[51] C. Bettini, X. S. Wang, and S. Jajodia, "Protecting privacy against location-based personal identification," in *Workshop on Secure Data Management*, pp. 185–199, Springer, 2005.

[52] J. Krumm, "Inference attacks on location tracks," in *International Conference on Pervasive Computing*, pp. 127–143, Springer, 2007.

[53] C. D. Cottrill *et al.*, "Location privacy preferences : A survey-based analysis of consumer awareness, trade-off and decision-making," *Transportation Research Part C : Emerging Technologies*, vol. 56, pp. 132–148, 2015.

[54] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pp. 71–80, ACM, 2005.

[55] E. Aïmeur, "Online privacy : risks, challenges, and new trends," in *International Conference on Risks and Security of Internet and Systems*, pp. 263–266, Springer, 2014.

[56] H. Fu, Y. Yang, N. Shingte, J. Lindqvist, and M. Gruteser, "A field study of run-time location access disclosures on android smartphones," *Proc. USEC*, vol. 14, 2014.

[57] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge, "Location disclosure to social relations : why, when, & what people want to share," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 81–90, ACM, 2005.

[58] K. Gordon, "Business site selection, location analysis, and gis," 2017.

[59] H. Xu, "M-commerce development in china-users' perspectives," *Journal of Technology Research*, vol. 5, p. 1, 2014.

[60] P. M. Adams, G. W. B. Ashwell, and R. Baxter, "Location-based services—an overview of the standards," *BT Technology Journal*, vol. 21, no. 1, pp. 34–43, 2003.

[61] M. L. Damiani, "Location privacy models in mobile applications : conceptual view and research directions," *GeoInformatica*, vol. 18, no. 4, pp. 819–842, 2014.

[62] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework : supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering*, vol. 16, no. 1, pp. 3–32, 2011.

[63] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *International conference on pervasive computing*, pp. 152–170, Springer, 2005.

[64] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proceedings of the 1st international conference on Mobile systems, applications and services*, pp. 31–42, ACM, 2003.

[65] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," *IEEE transactions on knowledge and data engineering*, vol. 19, no. 12, pp. 1719–1733, 2007.

[66] T. Xu and Y. Cai, "Location anonymity in continuous location-based services," in *Proceedings of the 15th annual ACM international symposium on Advances in geographic information systems*, p. 39, ACM, 2007.

[67] P. Samarati, "Protecting respondents identities in microdata release," *IEEE transactions on Knowledge and Data Engineering*, vol. 13, no. 6, pp. 1010–1027, 2001.

[68] C.-Y. Chow, M. F. Mokbel, J. Naps, and S. Nath, "Evaluation of range nearest-neighbor queries with quality guarantee," in *In Proceedings of the International Symposium on Spatial and Temporal Databases*, Citeseer, 2009.

[69] H. Hu and D. L. Lee, "Range nearest-neighbor query," *IEEE Transactions on Knowledge and Data Engineering*, vol. 18, no. 1, pp. 78–91, 2005.

[70] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper : A privacy-aware location-based database server," in *2007 IEEE 23rd International Conference on Data Engineering*, pp. 1499–1500, IEEE, 2007.

[71] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive : anonymous location-based queries in distributed mobile systems," in *Proceedings of the 16th international conference on World Wide Web*, pp. 371–380, ACM, 2007.

[72] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Mobihide : a mobilea peer-to-peer system for anonymous location-based queries," in *International Symposium on Spatial and Temporal Databases*, pp. 221–238, Springer, 2007.

[73] X. Lu and M. Au, "An introduction to various privacy models," in *Mobile Security and Privacy*, pp. 235–245, Elsevier, 2017.

[74] P. Shankar, V. Ganapathy, and L. Iftode, "Privately querying location-based services with sybilquery," in *Proceedings of the 11th international conference on Ubiquitous computing*, pp. 31–40, ACM, 2009.

[75] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *International Conference on Pervasive Computing*, pp. 390–397, Springer, 2009.

[76] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. Di Vimercati, and P. Samarati, "Location privacy protection through obfuscation-based techniques," in *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 47–60, Springer, 2007.

[77] M. L. Damiani, E. Bertino, and C. Silvestri, "Protecting location privacy against spatial inferences : the probe approach," in *Proceedings of the 2nd SIGSPATIAL ACM GIS 2009 International Workshop on Security and Privacy in GIS and LBS*, pp. 32–41, ACM, 2009.

[78] J. Xu, X. Tang, H. Hu, and J. Du, "Privacy-conscious location-based queries in mobile environments," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 3, pp. 313–326, 2009.

[79] C. Bettini, S. Mascetti, X. S. Wang, D. Freni, and S. Jajodia, "Anonymity and historical-anonymity in location-based services," in *Privacy in location-based applications*, pp. 1–30, Springer, 2009.

[80] Z. Sahnoune, "Vers une plateforme holistique de protection de la vie privée dans les services géodépendants," 2018.

[81] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on*, pp. 88–97, IEEE, 2005.

[82] M. L. Yiu, C. S. Jensen, X. Huang, and H. Lu, "Spacetwist : Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services," in *2008 IEEE 24th International Conference on Data Engineering*, pp. 366–375, IEEE, 2008.

[83] G. Ghinita, "Privacy for location-based services," *Synthesis Lectures on Information Security, Privacy, & Trust*, vol. 4, no. 1, pp. 1–85, 2013.

[84] J. Domingo-Ferrer, S. Martínez, D. Sánchez, and J. Soria-Comas, "Co-utility : self-enforcing protocols for the mutual benefit of participants," *Engineering Applications of Artificial Intelligence*, vol. 59, pp. 148–158, 2017.

[85] T. Peng, Q. Liu, D. Meng, and G. Wang, "Collaborative trajectory privacy preserving scheme in location-based services," *Information Sciences*, vol. 387, pp. 165–179, 2017.

[86] R. Shokri, P. Papadimitratos, G. Theodorakopoulos, and J.-P. Hubaux, "Collaborative location privacy," in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, pp. 500–509, IEEE, 2011.

[87] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J.-P. Hubaux, "Hiding in the mobile crowd : Locationprivacy through collaboration," *IEEE transactions on dependable and secure computing*, vol. 11, no. 3, pp. 266–279, 2013.

[88] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *2011 IEEE symposium on security and privacy*, pp. 247–262, IEEE, 2011.

[89] C.-Y. Chow and M. F. Mokbel, "Trajectory privacy in location-based services and data publication," *ACM Sigkdd Explorations Newsletter*, vol. 13, no. 1, pp. 19–29, 2011.

[90] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.

[91] A. Solanas, J. Domingo-Ferrer, and A. Martínez-Ballesté, "Location privacy in location-based services : Beyond ttp-based schemes," in *Proceedings of the 1st international workshop on privacy in location-based applications (PILBA)*, pp. 12–23, 2008.

[92] T. Wang and L. Liu, "From data privacy to location privacy," in *Machine Learning in Cyber Trust*, pp. 217–246, Springer, 2009.

[93] A. Pingley, N. Zhang, X. Fu, H.-A. Choi, S. Subramaniam, and W. Zhao, "Protection of query privacy for continuous location based services," in *2011 Proceedings IEEE INFOCOM*, pp. 1710–1718, IEEE, 2011.

[94] D. Quercia, I. Leontiadis, L. McNamara, C. Mascolo, and J. Crowcroft, "Spotme if you can : Randomized responses for location obfuscation on mobile phones," in *2011 31st International Conference on Distributed Computing Systems*, pp. 363–372, IEEE, 2011.

[95] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services : anonymizers are not necessary," in *Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, pp. 121–132, ACM, 2008.

[96] L. Zhang, Y. Li, L. Wang, J. Lu, P. Li, and X. Wang, "An efficient context-aware privacy preserving approach for smartphones," *Security and Communication Networks*, vol. 2017, 2017.

[97] M. L. Damiani, E. Bertino, C. Silvestri, *et al.*, "The probe framework for the personalized cloaking of private locations.," *Trans. Data Privacy*, vol. 3, no. 2, pp. 123–148, 2010.

[98] C. Parent, S. Spaccapietra, C. Renso, G. Andrienko, N. Andrienko, V. Bogorny, M. L. Damiani, A. Gkoulalas-Divanis, J. Macedo, N. Pelekis, *et al.*, "Semantic trajectories modeling and analysis," *ACM Computing Surveys (CSUR)*, vol. 45, no. 4, p. 42, 2013.

[99] C.-W. Chan and C.-C. Chang, "A scheme for threshold multi-secret sharing," *Applied Mathematics and Computation*, vol. 166, no. 1, pp. 1–14, 2005.

[100] A. Gutscher, "Coordinate transformation-a solution for the privacy problem of location based services?," in *Proceedings 20th IEEE International Parallel & Distributed Processing Symposium*, pp. 7–pp, IEEE, 2006.

[101] T. Hashem, L. Kulik, and R. Zhang, "Privacy preserving group nearest neighbor queries," in *Proceedings of the 13th International Conference on Extending Database Technology*, pp. 489–500, ACM, 2010.

[102] C. S. Jensen, H. Lu, and M. L. Yiu, "Location privacy techniques in client-server architectures," in *Privacy in location-based applications*, pp. 31–58, Springer, 2009.

[103] A. Patel and E. Palomar, "Privacy preservation in location-based mobile applications : research directions," in *2014 Ninth International Conference on Availability, Reliability and Security*, pp. 227–233, IEEE, 2014.

[104] F. Groschupp, "Location privacy preserving mechanisms," *Future Internet (FI) and Innovative Internet Technologies and Mobile Communication (IITM) Focal Topic : Advanced Persistent Threats*, vol. 9, 2017.

[105] A. R. Beresford and F. Stajano, "Mix zones : User privacy in location-aware services," in *IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second*, pp. 127–131, IEEE, 2004.

[106] B. Palanisamy and L. Liu, "Mobimix : Protecting location privacy with mix-zones over road networks," in *2011 IEEE 27th International Conference on Data Engineering*, pp. 494–505, IEEE, 2011.

[107] S. Mascetti, D. Freni, C. Bettini, X. S. Wang, and S. Jajodia, "Privacy in geo-social networks : proximity notification with untrusted service providers and curious buddies," *The VLDB Journal—The International Journal on Very Large Data Bases*, vol. 20, no. 4, pp. 541–566, 2011.

[108] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on encrypted databases," in *Proceedings of the 2009 ACM SIGMOD International Conference on Management of data*, pp. 139–152, ACM, 2009.

[109] H. Hu, J. Xu, C. Ren, and B. Choi, "Processing private queries over untrusted data cloud through privacy homomorphism," in *2011 IEEE 27th International Conference on Data Engineering*, pp. 601–612, IEEE, 2011.

[110] K. P. Puttaswamy, S. Wang, T. Steinbauer, D. Agrawal, A. El Abbadi, C. Kruegel, and B. Y. Zhao, "Preserving location privacy in geosocial applications," *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 159–173, 2012.

[111] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database protection," in *International Symposium on Spatial and Temporal Databases*, pp. 98–116, Springer, 2009.

[112] M. Gruteser and B. Hoh, "On the anonymity of periodic location samples," in *International Conference on Security in Pervasive Computing*, pp. 179–192, Springer, 2005.

[113] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information : k-anonymity and its enforcement through generalization and suppression," tech. rep., technical report, SRI International, 1998.

[114] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "l-diversity : Privacy beyond k-anonymity," in *22nd International Conference on Data Engineering (ICDE'06)*, pp. 24–24, IEEE, 2006.

[115] F. Anuar and U. Gretzel, "Privacy concerns in the context of location-based services for tourism," in *ENTER 2011 Conference*, 2011.

[116] J. V. Chen, W. Ross, and S. F. Huang, "Privacy, trust, and justice considerations for location-based mobile telecommunication services," *info*, vol. 10, no. 4, pp. 30–45, 2008.

[117] M. L. Yiu, C. S. Jensen, J. Møller, and H. Lu, "Design and analysis of a ranking approach to private location-based services," *ACM Transactions on Database Systems (TODS)*, vol. 36, no. 2, p. 10, 2011.

[118] G. Ghinita, M. L. Damiani, C. Silvestri, and E. Bertino, "Preventing velocity-based linkage attacks in location-aware applications," in *Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pp. 246–255, ACM, 2009.

[119] S. Saravanan and B. S. Ramakrishnan, "Preserving privacy in the context of location based services through location hider in mobile-tourism," *Information Technology & Tourism*, vol. 16, no. 2, pp. 229–248, 2016.

[120] J. Um, H. Kim, Y. Choi, and J. Chang, "A new grid-based cloaking algorithm for privacy protection in location-based services," in *High Performance Computing*

and Communications, 2009. HPCC'09. 11th IEEE International Conference on, pp. 362–368, IEEE, 2009.

[121] H. Lee, B.-S. Oh, H.-i. Kim, and J. Chang, "Grid-based cloaking area creation scheme supporting continuous location-based services," in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, pp. 537–543, ACM, 2012.

[122] I. Memon, "Authentication user's privacy : an integrating location privacy protection algorithm for secure moving objects in location based services," *Wireless Personal Communications*, vol. 82, no. 3, pp. 1585–1600, 2015.

[123] T.-H. You, W.-C. Peng, and W.-C. Lee, "Protecting moving trajectories with dummies," in *Mobile Data Management, 2007 International Conference on*, pp. 278–282, IEEE, 2007.

[124] H. Samet, *The design and analysis of spatial data structures*, vol. 85. Addison-Wesley Reading, MA, 1990.

[125] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity : Architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1–18, 2007.

[126] C. Zhang and Y. Huang, "Cloaking locations for anonymous location based services : a hybrid approach," *GeoInformatica*, vol. 13, no. 2, pp. 159–182, 2009.

[127] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, "Casper* : Query processing for location services without compromising privacy," *ACM Transactions on Database Systems (TODS)*, vol. 34, no. 4, p. 24, 2009.

[128] M. L. Damiani, E. Bertino, and C. Silvestri, "Protecting location privacy through semantics-aware obfuscation techniques," in *IFIP International Conference on Trust Management*, pp. 231–245, Springer, 2008.

[129] R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J.-P. Hubaux, "Unraveling an old cloak : k-anonymity for location privacy," in *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, pp. 115–118, ACM, 2010.

[130] M. Xue, P. Kalnis, and H. K. Pung, "Location diversity : Enhanced privacy protection in location based services," in *International Symposium on Location- and Context-Awareness*, pp. 70–87, Springer, 2009.

[131] A. Aloui, O. Kazar, S. Bourekkache, and F. Omary, "An efficient approach for privacy-preserving of the client's location and query in m-business supplying lbs services," *International Journal of Wireless Information Networks*, pp. 1–22.

[132] R. Gupta and U. P. Rao, "An exploration to location based service and its privacy preserving techniques : a survey," *Wireless Personal Communications*, vol. 96, no. 2, pp. 1973–2007, 2017.

[133] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive computing*, vol. 2, no. 1, pp. 46–55, 2003.

[134] C. Piao, S. Dong, and L. Cui, "A novel scheme on service recommendation for mobile users based on location privacy protection," in *e-Business Engineering (ICEBE), 2013 IEEE 10th International Conference on*, pp. 300–305, IEEE, 2013.

[135] H. Lu, C. Jensen, and M. Yiu, "A3d : Anonymity area aware, dummy-based location privacy in mobile services," *Proc. Data Eng. for Wireless and Mobile Access (MobiDE'08)*, 2008.

[136] Y. H. Gustav, Y. Wang, M. K. Domenic, F. Zhang, and I. Memon, "Velocity similarity anonymization for continuous query location based services," in *2013 International conference on computational problem-solving (ICCP)*, pp. 433–436, IEEE, 2013.

[137] H. Hu and J. Xu, "Non-exposure location anonymity," in *2009 IEEE 25th International Conference on Data Engineering*, pp. 1120–1131, IEEE, 2009.

[138] C.-Y. Chow, M. F. Mokbel, J. Bao, and X. Liu, "Query-aware location anonymization for road networks," *GeoInformatica*, vol. 15, no. 3, pp. 571–607, 2011.

[139] Netbeans, "Qu'est ce que NetBeans ?," 2011.

[140] L. Stenneth and P. Yu, "Global privacy and transportation mode homogeneity anonymization in location based mobile systems with continuous queries," in *2010 6th International Conference on Collaborative Computing : Networking, Applications and Worksharing (CollaborateCom 2010)*, pp. 1–10, IEEE, 2010.

[141] X. Pan, X. Meng, and J. Xu, "Distortion-based anonymity for continuous queries in location-based mobile services," in *Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pp. 256–265, ACM, 2009.