République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA

Faculté des Sciences Exactes
Département d'Informatique

Mémoire

Présenté par

BENSIMESSAOUD Sihem

Pour l'obtention du diplôme de Magister

Filière : Informatique

Option : Cloud Computing

Thème

Préservation de la confidentialité des informations personnelles dans la publication des réseaux sociaux

Soutenu le : 29/09/2016 Devant le Jury composé de :

Nom et Prénom	Grade		
M. TARI Abdelkamel	Professeur	Université de Bejaïa	Président
M. BADACHE Nadjib	Professeur	CERIST, Alger	Rapporteur
M. BOUKERRAM Abdallah	Professeur	Université de Bejaïa	Examinateur
Mme BENZAID Chafika	MCA	USTHB, Alger	Invitée
Mme BENMEZIANE Souad	CR	CERIST	Invitée

Année Universitaire : 2015/2016

Résumé

Aujourd'hui, de plus en plus les données du réseau social sont rendues publiquement disponibles à des fins d'analyse des données. Bien que cette analyse soit importante pour les chercheurs, il peut y avoir un risque de violation de la vie privée des utilisateurs constituant ce réseau social. Avec peu de connaissances locales sur les individus dans un réseau social, un adversaire peut réaliser différents types d'attaques. Parmi les informations que peut collecter un adversaire sur une victime cible, nous trouvons « le voisinage », c'est à dire, quels sont les voisins de la victime et comment ces voisins sont connectés. Cette information pourra ainsi aider l'adversaire à identifier la personne même si d'autres informations d'identification sont supprimées. Dans notre travail, nous avons fait une étude détaillée de l'approche d'anonymisation proposée par Zhou et Pei [54] contre les attaques de voisinage et nous avons pu identifier quelques faiblesses concernant l'altération des propriétés structurelles du graphe anonymisé résultant. Ceci nous a conduit à proposer une nouvelle approche d'anonymisation des graphes sociaux à publier tout en maintenant l'utilité des données du réseau qui reflète les propriétés structurelles du graphe original notamment APL. La solution consiste à implémenter le modèle « k-voisinage » pour garantir que tout individu ne peut pas être identifié correctement dans le graphe social anonymisé avec une probabilité supérieure à 1/k, tel que pour chaque sommet appartenant au graphe, il existe au moins (k-1) autres sommets ayant des voisinages isomorphes. Le but de l'approche proposée est d'une part de protéger les données publiées contre les attaques de voisinages et de préserver l'utilité du graphe social anonymisé d'autre part.

Remerciements

Au nom d'ALLAH le tous Miséricordieux et que le salut soit sur notre prophète Mohamed aalayh Elssalet wa Elssalem.

Je remercie ALLAH, Le Tout Puissant, pour son aide et sa protection, et de m'avoir donné la patience et le courage pour accomplir ce travail.

Ce mémoire est le résultat d'un effort. Cet effort n'aurait pas pu aboutir sans la contribution d'un nombre de personnes. Ainsi se présente l'occasion de les remercier.

J'exprime ma profonde gratitude, mes remerciements, les plus vifs à Monsieur le Directeur du CERIST ***N.BADACHE*** *de m'avoir offert l'opportunité de suivre une formation en magistère.*

Je tiens à remercier vivement et tout particulièrement Madame ***S.BENMEZIANE*** *d'avoir accepté de suivre mon travail et pour ses précieux conseils et d'avoir été tout le temps disponible et à l'écoute. Je lui suis reconnaissante de m'avoir permis de travailler avec elle pendant mon projet d'Ingéniorat et ensuite pendant mon Magistère, de m'avoir initié à l'univers de la sécurité informatique et d'être pour moi vraiment un exemple de rigueur tout au long de la réalisation de ce travail.*

J'adresse mes vifs remerciements également à Monsieur ***A.TARI*** *pour l'honneur qu'il a bien voulu m'accordé en présidant le jury de ce travail.*

Je remercie ***Mme C. BENZAID*** *d'avoir accepté d'évaluer ce travail.*

Je remercie l'intérêt porté par Monsieur ***A. BOUKERRAM*** *d'avoir accepté d'être parmi le jury.*

J'adresse mes remerciements à Monsieur le Professeur ***N. BADACHE*** *d'avoir accepté d'encadrer ce travail et pour ses conseils et orientations.*

Je remercie notre Responsable de la division Sécurité Monsieur ***O. NOUALI*** *pour sa bienveillance.*

Je remercie mon marie qui m'a toujours soutenue du bon cœur et pour ses conseils et orientations.

Je tiens à exprimer ma très grande affection à mes chers parents et mes proches pour leurs encouragements, leur patience et leur grand soutien durant toutes ces années d'études.

Je remercie également Monsieur ***BENDJOUDI*** *qui m'a donné l'occasion de travailler sur le cluster IbnBadis du notre centre de calcul.*

Je remercie également le service Formation du CERIST de nous avoir prodigué un excellent environnement de travail.

A tous mes amis et camarades pour leurs encouragements et leur précieux soutien.

Dédicaces

Je remercie Dieu qui m'a permis de mener à bien mon projet.

À ma très chère mère « Zineb » et à mon très cher père « Laïd » qui n'ont pas cessé de me combler par leur amour et leur tendresse et qui m'ont donné un magnifique modèle de labeur et de persévérance dont le rêve était toujours de me voir réussir. J'espère qu'ils trouveront dans ce travail toute ma reconnaissance et tout mon amour.

A mon cher mari « Mustapha » qui m'a toujours soutenu, m'a encouragé pour bien mener ce travail et qui était vraiment patient avec moi.

, ma princesse « Lina Sirine » qu'ALLAH la protège, elle était toujours avec moi pendant tous mon travail.

A mes chères sœurs « Soumia », « Roukia », « Amina » qui m'ont toujours soutenu ainsi que mes deux frères « Abdelfateh » et « Lyess ».

A ma belle-famille qui m'a tant encouragé, j'ai vraiment eu la chance de vous avoir : à mon beau-père et ma belle-mère rabby yarehameha ainsi que mes très chères belles sœurs: « Dalila », « Nawel» et « Samah », mes beaux-frères « Mehdi » ainsi que « Ahmed » et sa femme « Asma » et leur adorable enfant « Iyad ».

A Mes Tantes « Rachida », « Nouara » et « Saltanna » qui m'ont toujours aidé dans mes choix et pour leurs conseils et leurs prières. Je leur souhaite la bonne santé.

A ma très chère grand-mère ainsi que mon grand-père et toute ma famille.

A notre cher pays et à nos frères dans tout le monde musulman, que Dieu les protège.

A ma très chère amie et sœur, mon magnifique ancien binôme du cycle d'ingéniorat et ma collègue de travail dans le même bureau « Mina ».

A tous mes amis (es) qui n'ont jamais manqué de témoigner leur estime à mon égard spécialement « Karima », « Amel », « ElBatoul », « Hamida », « Kaho », « Wiza », « Mounia », « Ghania », « Noussaiba », « Ikram », « Sabira » et « Nesrine ».

À tous ceux que j'aime

J'exprime ma profonde et sincère gratitude ; je leur dédie ce modeste travail.

En raison de l'augmentation de la popularité des réseaux sociaux au cours des dernières années, un grand nombre de personnes y souscrivent. Cela a généré une grande quantité de données d'utilisateurs qui sont recueillies et conservées par les fournisseurs de services de réseaux sociaux. Cette énorme quantité de données a attiré l'intérêt de la communauté de recherche, les annonceurs tiers, et les services gouvernementaux dans le but de l'analyse des données pour obtenir des informations utiles tels que le comportement de l'utilisateur, la croissance de la communauté, la propagation d'une maladie, etc.

Aujourd'hui, de plus en plus les données des réseaux sociaux sont publiées d'une manière ou d'une autre à des tiers, tels que les développeurs d'applications, les chercheurs, les sociologues et les sociétés commerciales. Ces données sont très précieuses pour ces tiers, puisqu'ils peuvent les analyser pour en extraire les informations dont ils ont besoin pour leurs objectifs particuliers. Par exemple, une entreprise peut utiliser les données qui forment la base de profils des clients, pour promouvoir ses produits à ses clients à travers un système de recommandation en ligne et peut même utiliser les liens entre les utilisateurs du réseau social pour élargir leurs bases de clients. Les employeurs peuvent également utiliser les réseaux sociaux pour identifier des clients potentiels ou recruter des employés candidats. En effet, selon les statistiques publiées dans Time Magazine en 2007, 12% des employeurs aux États-Unis utilisaient déjà les sites de réseautage social populaires tels que MySpace et Facebook pour étudier les profils de certains employés potentiels. Les sociologues, à leur tour, peuvent analyser ces données pour mieux comprendre l'évolution des communautés sociales dans le monde physique.
Certains réseaux sociaux recueillent des informations confidentielles des individus et/ou des relations confidentielles entre les individus. Par exemple, PatientsLikeMe[1], Rareshare[2], et DailyStrength[3] sont des réseaux sociaux dans le domaine de soins de la santé qui créent des communautés de patients pour différentes maladies. En conséquence, la vie privée dans les réseaux sociaux est devenue une préoccupation sérieuse en particulier lorsque les données du réseau social sont publiées.

Conceptuellement, Les données d'un réseau social peuvent être représentées sous forme d'un graphe social, où les sommets représentent les individus et les arêtes représentent les relations entre ces individus. En plus de sommets et d'arêtes, des informations supplémentaires sur les individus et leurs relations peuvent être représentées par des étiquettes ou labels. Les labels de sommets peuvent représenter les attributs d'une personne, comme l'identité ou le genre. Les labels d'une arête peuvent représenter les attributs sur les relations, y compris la nature des relations, par exemple, l'amitié ainsi que le poids de relations qui peut décrire par exemple le degré d'une amitié.
Puisque certaines données représentées sur le graphe social peuvent contenir beaucoup de détails privés et sensibles sur les individus (par exemple, le salaire, la maladie, la connexion à un groupe spécifique de personnes, etc.), la publication de ces données dans leur forme brute peut violer la vie privée des individus. Par conséquent, préserver la vie privée tout en publiant les données du réseau social devient un des problèmes principaux pour les utilisateurs du réseau et un domaine de recherche très important.

[1] http://www.patientslikeme.com, depuis 2005.
[2] http://www.rareshare.org, depuis 2008.
[3] http://www.dailystrength.org, depuis 2006.

Beaucoup de travaux ont été réalisés pour la préservation des informations privées lors de la publication des données du réseau social. Dans la littérature [62], Hay et al ont proposé l'anonymisation naïve, qui remplace les attributs d'identification des individus dans un réseau avec des identifiants aléatoires avant de publier les données. Bien que le réseau naïvement anonymisé permet une analyse utile et les propriétés globales du réseau sont conservées, cette approche simple peut être insuffisante puisqu'un adversaire pourrait encore ré-identifier le nœud d'une personne cible sur le graphe anonymisé en exploitant des connaissances préalablement collectées. Il peut également apprendre l'existence d'une relation sociale entre deux nœuds ré-identifiés ou encore utiliser la structure du graphe elle-même pour déduire la valeur de certains attributs sensibles. L'anonymisation est un processus crucial pour assurer que les données publiées du réseau social ne révèlent pas des informations sensibles des utilisateurs. Plusieurs approches d'anonymisation pour les bases de données ont été adoptées pour anonymiser les données des réseaux sociaux et prévenir les différentes attaques possibles sur ces réseaux.

Dans notre travail, nous identifions un type important d'attaques contre la vie privée dans les réseaux sociaux: « les attaques de voisinage ». Si un adversaire possède une certaine connaissance sur les voisins d'une victime cible et les relations entre ces voisins, la victime peut être ré-identifiée même si l'identité de la victime est protégée à l'aide des techniques conventionnelles d'anonymisation.
L'étude approfondie de l'attaque de voisinage, nous a permis de bien comprendre les approches d'anonymisation proposées contre ces attaques. Elles se basent sur le principe de l'ajout des liens pour avoir des voisinages isomorphes et préservent ainsi considérablement la vie privée. Cependant, ces approches peuvent modifier de manière significative les propriétés du graphe original et peuvent causer des erreurs significatives dans certaines tâches d'analyse des propriétés structurelles telles que la mesure de la distance moyenne APL, le diamètre, le rayon, etc.
Dans ce contexte, l'objectif de notre travail est de proposer une nouvelle approche d'anonymisation dans le but de prévenir les attaques de voisinage tout en préservant le mieux possible la distance sociale sur laquelle se basent d'autres propriétés structurelles notamment APL.
La solution consiste à adopter le modèle « k-voisinage » pour garantir que tout individu ne puisse pas être identifié correctement dans le graphe social anonymisé avec une probabilité supérieure à 1/k. Ainsi, pour chaque sommet appartenant au graphe, il existera au moins (k-1) autres sommets ayant des voisinages isomorphes. Nous proposons pour améliorer la préservation de la distance l'ajout de faux nœuds en plus de l'ajout de liens. Il est intéressant de comparer les résultats obtenus à l'issue de l'anonymisation avec le modèle déjà proposé par Zhou et Pei [54]. Plus précisément, nous observons comment les caractéristiques telles que l'APL, le rayon et le diamètre sont préservés par l'outil d'anonymisation du graphe social développé. Les différents tests sont effectués sur un ensemble de graphes sociaux synthétiques et réels.

Le présent document est structuré de la manière suivante :

Dans le premier chapitre, nous présentons les concepts des réseaux sociaux ainsi que les menaces de sécurité dans ces réseaux.

Nous introduisons dans le second chapitre le problème de la préservation de la vie privée des utilisateurs des réseaux sociaux lorsque ces données sont publiées. Plusieurs questions clés sont abordées comme le compromis entre la vie privée et le partage des informations en

public et les attaques sur le graphe publié. Nous décrivons aussi les approches d'anonymisation proposées dans la littérature.

Le troisième chapitre sera consacré à la description de l'approche d'anonymisation proposée pour prévenir « l'attaque de voisinage » quand les données du réseau social sont publiées. La méthode d'anonymisation de deux voisinages, la méthode de vérification de la similarité et d'anonymisation de deux composantes ainsi que la méthode d'ajout de nœuds seront présentés dans ce chapitre.

Dans le quatrième chapitre, nous évaluons la solution proposée en comparant les résultats de l'algorithme déjà proposé par Zhou et Pei que nous avons implémenté, avec les observations expérimentales de notre nouvel algorithme.

Nous achèverons ce mémoire par une conclusion générale ainsi que quelques perspectives de ce travail seront proposées.

1 Introduction

Avec la croissance rapide des techniques de communication d'Internet, le World Wide Web est devenu une plate-forme très importante pour les utilisateurs pour interagir les uns avec les autres. Grâce à ces plates-formes, les utilisateurs peuvent facilement partager et diffuser des informations et des idées. Au cours des dernières années, un nouveau phénomène a été introduit à la société en ligne et qui a changé considérablement la façon dont les gens communiquent, partagent du contenu et surfent sur le web. Nous nous référons sans aucun doute au phénomène de réseau social. Ces réseaux peuvent être très bénéfiques pour les utilisateurs, car ils ont enlevé les frontières géographiques et économiques. En plus d'entrer en contact avec des amis et rester connectés et partager facilement et instantanément différentes informations comme les activités quotidiennes, voyages, photos, etc. à un coût beaucoup plus petit et avec moins d'effort, les réseaux sociaux peuvent être utilisés à des fins ciblés telles que l'éducation, la recherche d'emploi, et beaucoup plus. En effet, ces réseaux ont gagné une grande popularité et sont devenues une partie essentielle de la vie des utilisateurs.

L'énorme quantité d'informations générée par les utilisateurs du web à travers les réseaux sociaux n'a jamais été disponible auparavant et sont devenues des sources de choix pour extraire et analyser des réseaux sociaux de très grandes tailles. Dans le passé, pour étudier les relations, les comportements, les interactions, et les propriétés des groupes spécifiques de personnes, il était nécessaire de faire beaucoup d'efforts pour gagner quelques informations pas très détaillées [18], les discussions électroniques et la structure en hyperliens du web étaient les principales sources du web à disposition des chercheurs jusqu'à l'avènement du web 2.0. La popularité montante des outils collaboratifs du web 2.0 permet d'étudier de nouveaux réseaux à grande échelle avec des acteurs qui fournissent plus d'informations sur eux-mêmes mais également sur les personnes avec qui ils interagissent. En effet, l'émergence des réseaux sociaux en ligne, et l'énorme quantité d'activités diverses qui sont générés par leurs utilisateurs, l'information désirée est accessible beaucoup plus simplement et avec incomparablement plus de détails qu'auparavant par les chercheurs. Ceci a conduit à différents types de recherche avec différents objectifs [18]. Les avantages et les parties prenantes qui pourraient bénéficier d'avoir cette information ou d'avoir les résultats de leur analyse sont plusieurs, certains d'entre eux sont: les entreprises commerciales pour faire de la publicité et promouvoir leurs produits, les sociologues pour analyser le comportement et les caractéristiques des différentes sociétés, les employeurs pour acquérir des informations sur les demandeurs d'emploi, …etc. [18]

Cependant, cette facilité de communication et de partage d'information s'est avérée être une arme à double tranchant [46], ces réseaux peuvent également être une source de nombreuses menaces pour la sécurité de l'utilisateur. Compte tenu de la grande quantité de renseignements personnels qui sont partagés dans ces réseaux, protéger la vie privée des utilisateurs a émergé comme un problème important. Plusieurs menaces à la vie privée qui exploitent soit les données personnelles d'un utilisateur ou les vulnérabilités des réseaux sociaux existent comme le vol d'identité, le harcèlement et divers crimes cybernétiques. La vie privée est devenue une préoccupation principale pour ses utilisateurs. Par conséquent l'analyse et la compréhension de tels réseaux suscitent de vifs intérêts.

Dans les prochaines sections de ce chapitre, nous présentons les principaux concepts ou terminologies impliqués dans ce mémoire. Nous commençons par la définition du concept des réseaux sociaux en introduisant brièvement les réseaux sociaux en ligne et les différents

médias sociaux sur Internet ainsi que les sites de réseautage social et ceci dans les sections 2, 3, 4 et 5. La sixième section donnera un aperçu sur quelques sujets de recherche dans le domaine des réseaux sociaux. La section 7 décrit la modélisation mathématique d'un réseau social, qui se fait par des moyens de la théorie des graphes, rappelons quelques notions de la théorie des graphes adaptées aux réseaux sociaux. Ensuite nous présentons les différentes caractéristiques communes des réseaux sociaux ainsi que le concept d'analyse des réseaux sociaux et cela dans les sections 8 et 9 respectivement. Nous discuterons dans la section 10 les différents problèmes liés à la sécurité dans ces réseaux et nous donnons un aperçu sur les menaces de sécurité les plus courantes ainsi que les solutions existantes contre ces menaces. Nous concluons le chapitre dans la section 11.

2 Définition des réseaux sociaux

Un réseau social est définit comme un ensemble d'acteurs ou entités sociales (Individus, groupes ou organisations) reliés par des interactions sociales. Ces interactions peuvent être de différentes natures : familiales, sentimentales (liens forts) ou plus distantes : affinité, relation d'affaire, de travail (liens faibles)… Elles peuvent se nouer à travers des contacts directs ou médiés technologiquement : échange d'emails, chats, réseaux sociaux, mondes virtuels… [1]. Le terme de réseau social provient de John Arundel Barnes en 1954, un anthropologue australien et britannique [44] et existait bien avant Internet.

Le terme de réseau social s'est élargi avec le temps et a pris de nouvelles proportions. On l'attribut désormais habituellement aux nombreux sites Internet qui se multiplient de jour en jour et qui sont caractérisés par le fait de rapprocher les individus via des interactions virtuelles [44].

Ainsi [2] distingue trois catégories de réseaux sociaux sur le web:

- Les réseaux sociaux inférés avec des techniques de web mining : citations entre pages personnels, PageRank, cooccurrence de noms.
- Les discussions électroniques : mails, chat, forum.
- Les applications sociales du web 2.0 : outils de publication (wiki, blog, news), sites de réseaux sociaux, sites de partage (contenu, produits, évènements, etc.) et jeux collaboratifs.

3 Les réseaux sociaux en ligne

Les réseaux sociaux en ligne (ou en anglais Online Social Networks ou OSN) est une expression numérique du réseau social [10], une plate-forme pour construire des réseaux sociaux ou des relations sociales entre les individus qui, par exemple, partagent des intérêts, des activités, des contexte ou des relations réelles [14]. Wellman [3] argumente que les relations en ligne forment des réseaux sociaux virtuels représentatifs des réseaux sociaux réels. En effet, ces réseaux virtuels sont créés à partir d'interactions initiées par des personnes physiques. Les réseaux sociaux virtuels offrent à l'internaute la possibilité d'être acteur d'Internet et plus seulement récepteur. Ils sont caractéristiques du web 2.0 dit collaboratif : chacun peut publier un contenu et réagir au contenu des autres. Apparus au début des années 2000, et ils connaissent un succès fulgurant sur Internet [10].

Il existe deux grands types de réseaux sociaux en ligne : [10]

1. Les réseaux sociaux généralistes : essentiellement utilisés pour créer des cercles d'amis et communiquer avec eux tels que Google+, Facebook.

2. Les réseaux à usage professionnel : tels que LinkedIn.

En termes d'appellation, il est exact d'utiliser l'expression "réseaux sociaux en ligne", mais par simplification ils sont appelés "les réseaux sociaux". Par la place qu'ils ont pris dans le paysage médiatique, le terme aussi de "médias sociaux" est utilisé pour les désigner. [10]

4 Les médias sociaux

L'expression « médias sociaux » recouvre les différentes activités qui intègrent la technologie, l'interaction sociale (entre individus ou groupes d'individus), et la création de contenu. Andreas Kaplan et Michael Haenlein définissent les médias sociaux comme « un groupe d'applications en ligne qui se fondent sur la philosophie et la technologie du net et permettent la création et l'échange du contenu généré par les utilisateurs » [43].

Depuis 2008 Fred Cavazza sur son blog [4] propose un panorama des médias sociaux. Il les a définis en 2009 comme suit: « Les médias sociaux désignent un ensemble de services permettant de développer des conversations et des interactions sociales sur ordinateur ou terminaux mobiles». La figure 1.1 rassemble la dernière version de son panorama « panorama des médias sociaux 2015 » qui s'organise autour de quatre grands usages : la publication, le partage, la discussion et le réseautage.

1. La publication avec les plateformes d'hébergement de blog (WordPress, Blogger, Live Journal , …), la nouvelle génération de services de publication minimalistes (Svbtle, Ghost), les wikis (Wikipedia, Wikia, Mahalo…) et les services intermédiaires de publication / partage comme Tumblr ;
2. Les services de partage « Sharing » pour publier et s'échanger des ressources. Comme le partage de photos (Flickr, Pinterest,…), de vidéos (YouTube, Dailymotion,…), de musique (SoundCloud, MySpace…), de liens (Delicious, Scoop.it), de lieux (Foursquare, Swarm), les applications mobiles (Instagram, Slingshot,…), les communautés d'acheteurs (TheFancy, Polyvore,…) ainsi que des communautés verticales comme ces trois-là dédiées aux designeurs (Behance, Dribbble, DeviantArt) ;

3. La discussion avec les plateformes conversationnelles (Quora, Disqus,…), les outils de communication grand public (Skype, Sina Weibo,…), les applications mobiles de communication (Facebook Groups, BlackBerry Messenger, Telegram …), et les outils de communication professionnels (Slack, Yammer, Chatter, …) ;
4. Le réseautage pour rechercher, se connecter et interagir avec des personnes avec les réseaux sociaux grand public (Tagged, Nextdoor, Notabli, Ello…) et leurs équivalents asiatiques et russes (Qzone, VKontakte, RenRen, …), les services de rencontre (Badoo, OKcupid…), les applications mobiles de rencontre (Tinder, Skout), et les réseaux sociaux BtoB (LinkedIn, Viadeo, Xing).

Au centre de cet écosystème, nous retrouvons Facebook et Twitter, puisque ils sont simplement en bout de chaine et concentrent / relayent toutes les interactions sociales qui sont faites sur les autres plateformes. Ces deux-là ne seraient pas aussi puissants sans les contenus

publiés et partagés au sein de cet écosystème. Deux plateformes emblématiques des médias sociaux, mais qui ont chacune des spécificités : Facebook est un portail, Twitter est un média. Au centre, nous allons également trouver toute une série d'applications mobiles. [4]

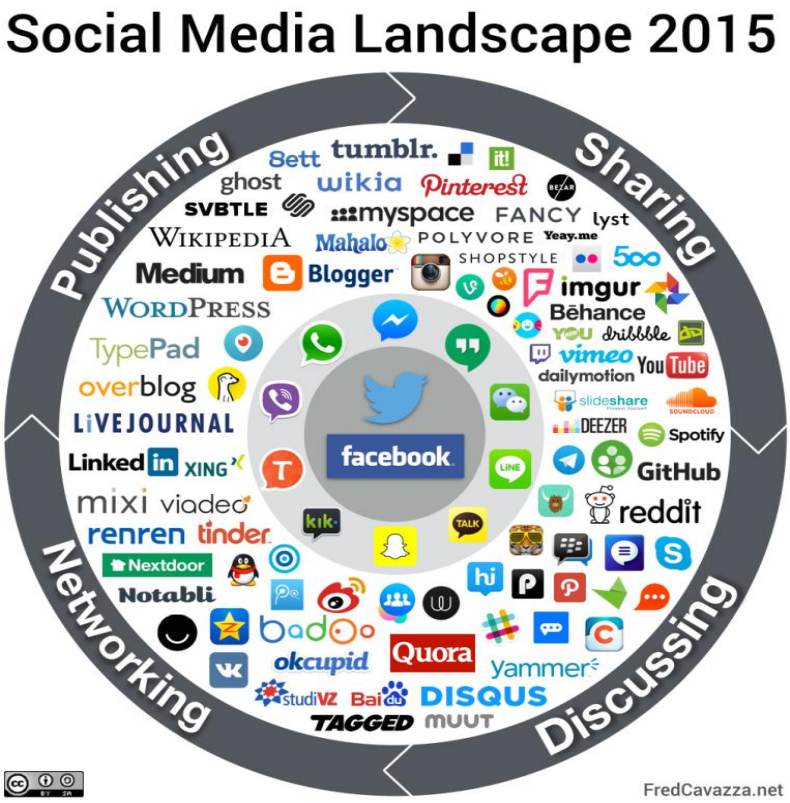


Figure 1.1: Panorama des Médias sociaux [4]

5 Les sites de réseautage social

Les sites de réseautage social (Social Networking Site ou SNS) comme Facebook, Twitter, LinkedIn, etc. ont gagné une popularité importante [11]. La participation des utilisateurs dans ces sites forme les réseaux sociaux en ligne où les utilisateurs sont représentés par une entité unique et personnelle (souvent appelé un profil), leurs liens sociaux (les utilisateurs qui sont des amis avec) et une variété de services supplémentaires. La plupart des services de réseaux sociaux sont basés sur le Web et fournissent des moyens pour que les utilisateurs interagissent sur Internet, tels que l'e-mail et la messagerie instantanée [14]. Ils fournissent des moyens puissants pour partager, organiser, et trouver de contenus et des contacts. La popularité de ces sites offre la possibilité d'étudier les caractéristiques des réseaux sociaux en ligne à grande échelle.

Dans cette section, nous introduisons le concept de site de réseautage social. Plus précisément, dans la première sous-section, nous donnons une brève définition des SNSs et dans la seconde sous-section, nous étudions les SNS bien connus et populaires et mettre en évidence les principales classifications des SNSs.

5.1 Définition d'un site de réseautage social SNS « Social Networking Site »

Sur les sites de réseautage social, un utilisateur peut créer une identité virtuelle et interagir en ligne avec d'autres utilisateurs. Par définition, les sites de réseaux sociaux sont des services web qui permettent à l'utilisateur de : [8]

(1) Construire un profil public ou semi-public dans le système,
(2) Articuler une liste d'autres utilisateurs avec lesquels il partage une connexion, (la nature et la nomenclature de ces relations peuvent varier d'un site à un autre),
(3) Voir et parcourir leurs liste de connexions et celles créées par d'autres dans le système.

Bien que cette définition ne contienne que des fonctions de base, les sites de réseautage social ont été enrichis par de nombreux autres services tels que le texte, photos, publication de vidéos et services de géolocalisation [8]. Avec l'augmentation du nombre de participants, ces réseaux deviennent de plus en plus complexes et peuvent facilement intégrer une vaste gamme de concepts sociologiques telles que l'amitié, le voisinage, la communauté, etc.

Une autre définition plus large a été proposée dans [11] :
Un site de réseautage social est un site Web qui permet aux utilisateurs de:

- **Se connecter** avec d'autres utilisateurs par « être ami avec » (Facebook), suivre (Twitter), souscrire (Youtube).
- **Interagir** avec le contenu posté par d'autres utilisateurs, par exemple en commentant, répondant ou en notant ce contenu.
- **Restreindre** leur propre contenu aux utilisateurs autorisés seulement.

5.2 Classification des sites de réseautage social

Les SNSs existants sont de nature très diverse et favorisent différents types d'interactions et d'activités. Selon la nature des relations sociales, les caractéristiques et la structure des SNSs, ils peuvent varier significativement les uns des autres. Par exemple, Sharma [56] fournit une liste complète de SNSs et les classifie en différentes catégories comme les livres, le réseautage d'affaires et professionnels, famille, amis, loisirs et intérêts, et médias, etc. Nations [67] résume les SNSs en trois grandes catégories : les sites à usage général, les sites de niche avec un thème spécifique et sites internationaux.
Comme notre principale préoccupation porte sur les questions de vie privée sur les SNSs, nous nous intéressons à la classification proposée par [11] basée sur deux critères: (1) comment ces sites affectent la vie privée de leurs utilisateurs et (2) les types d'informations échangées entre les utilisateurs.

5.2.1 SNSs personnels

Les SNSs personnels donnent la possibilité aux utilisateurs de se connecter et de communiquer avec des amis, des connaissances et la famille. Les utilisateurs mettent souvent une grande quantité de renseignements personnels sur leurs profils. Des exemples typiques de SNSs personnels incluent : Facebook[4], et Google+ [5] [11].

[4] https://Facebook.com
[5] http://plus.google.com

- Facebook, fondé par Mark zuckerberg, a été à l'origine conçu comme un site de réseautage social pour les étudiants de l'université d'harvard. Après sa diffusion à d'autres universités et à l'école secondaire, facebook a été ouvert au public en 2006. Selon [16] à partir d'octobre 2012, facebook avait 1 milliard de membres actifs dans le monde. Sur facebook, un utilisateur possédant un compte peut créer son profil et d'y publier des informations dont il peut contrôler la visibilité par les autres utilisateurs [11]. L'usage de ce réseau s'étend du simple partage d'informations d'ordre privé (par le biais de photographies, liens, textes, etc.) à la constitution de pages et de groupes visant à faire connaître des institutions, des entreprises ou des causes variées. L'intégralité des informations publiées sur ces deux supports (pages et groupes), à l'inverse du profil, peut être consultée par n'importe quel internaute sans qu'il soit nécessaire d'ouvrir un compte. Seuls les noms des membres du groupe ou de la page sont cachés [10].

- Google+ est un SNS exploité par Google, initialement lancé en Juin 2011 en format Beta, et plus tard rendu public en septembre 2011. Google+ intègre directement différents services sociaux de Google, tels que les Profils Google et Google Buzz, mais introduit également de nouvelles fonctionnalités telles que les cercles, Hangouts, Sparks et Huddles [11].

5.2.2 SNSs professionnels

Le but principal des SNSs professionnels est de connecter les utilisateurs avec des contacts professionnels, ainsi que de les aider à trouver un emploi ou chercher des employés. Par exemple, LinkedIn[6], et Xing[7] sont des sites web que les jeunes professionnels se joignent principalement pour accélérer leurs carrières. Les informations sur ces SNSs incluent souvent des contacts d'affaires, l'expertise, la recommandation et les offres d'emploi. La plupart des SNSs professionnels sont structurés de telle manière qu'ils peuvent être utilisés pour gérer les relations avec les clients [11].

- LinkedIn est un SNS orienté commercial ou métier dans lequel les membres invitent d'autres personnes à leurs «connexions» (en contraste avec le terme «amis» utilisé par Facebook) [11]. LinkedIn est en même temps un système de gestion des contacts et un réseau social. Il permet de construire et d'agréger son réseau professionnel. Il se définit comme un réseau de connaissances qui facilite le dialogue entre professionnels. Pour ses membres, c'est aussi un outil de gestion de réputation en ligne.

- Xing est un SNS pour les professionnels qui a plus de 11,4 millions de membres dans le monde (à partir de Septembre 2011). Les membres de Xing peuvent se rencontrer et échanger des vues avec environ 50 000 spécialistes du groupe, tout en rencontrant d'autres membres dans des événements de réseautage [11].

[6] http://LinkedIn.com
[7] http://xing.com

5.2.3 Loisirs et Intérêts

Ces SNSs correspondent principalement à des endroits où les utilisateurs partagent leurs hobbies et intérêts tels que les films (Flixster [8]) et la musique (Last.fm[9]). Dans ces sites, la plupart des informations affichées ne peuvent pas être utilisées pour identifier directement un utilisateur et sont souvent considéré comme moins sensibles par rapport à sa vie privée.

- Last.fm s'appelle un site de musique social. Il permet aux utilisateurs enregistrés de créer leur propre station de radio qui apprend les goûts musicaux d'une personne et suggère de nouvelles mélodies personnalisées à l'intérêt de l'utilisateur. En outre, les utilisateurs peuvent écouter les stations de radio des amis et d'autres utilisateurs de Last.fm [11].

5.2.4 SNS fonctionnels

Les SNS fonctionnels offrent différentes fonctionnalités spécifiques tels que les blogs, partage de photos, partage de statut, bookmarking social et critique de produits. Souvent, ces SNS ne capturent pas nécessairement des informations démographiques mais plutôt une grande quantité de renseignements personnels tels que les images. Des exemples de SNS fonctionnels comprennent LiveJournal[10](blog), Picasa [11] et Flickr [12] (partage de photos et de vidéos), Digg [13] et StumbleUpon [14] (bookmarking social), Consmr [15] (critiques sur les produits), etc. [11].

- Livejournal est une communauté virtuelle où les internautes peuvent gérer un blog ou un journal. En Février 2012, plus de 35 millions de comptes existaient sur LiveJournal avec cependant seulement 1,9 millions listés comme « actif»[16].

- Twitter est en même temps un service de micro-blogage et un SNS qui permet à ses utilisateurs d'envoyer et de lire des messages textuels courts qui peuvent contenir jusqu'à 140 caractères appelés «tweets». Twitter a été créé en Mars 2006 par Jack Dorsey et lancé la même année en Juillet. Il est rapidement devenu une plate-forme populaire avec plus de 300 millions d'utilisateurs à partir de Mars 2011[17], selon [15] il a reconnue en 2012 une grande augmentation du nombre de tweets publiés par jour (environ 340 millions de tweets par jour).

- YouTube est un site de partage de données, qui permet l'hébergement de vidéos, sur lequel les utilisateurs peuvent envoyer, visualiser et partager des séquences vidéo.

[8] http://flixter.com
[9] http://last.fm
[10] http://livejournal.com
[11] http://picasa.com
[12] http://flickr.com
[13] http://digg.com
[14] http://stumbleupon.com
[15] http://consmr.com
[16] http://www.livejournal.com/stats.bml
[17] http://yearinreview.twitter.com/en/whojoined.html

6 Quelques axes de recherche dans le domaine des réseaux sociaux

Les réseaux sociaux en ligne sont déjà au cœur de certains sites web très populaires. Le réseautage social joue un rôle important dans l'interaction en ligne personnelle et commerciale. L'émergence de ces réseaux et la participation croissante des personnes à des activités dans ces sites ainsi que l'énorme quantité d'informations diverses comme les interactions, les commentaires, les intérêts et les différents types de contenus publiés qui sont générés par les utilisateurs ont attiré les chercheurs et d'autres parties pour avoir accès à ces informations. Cette information n'a jamais été disponible avec un volume, un détail, et une facilité et une rapidité d'accès si énormes auparavant. Ils sont devenus des sources de choix pour extraire et analyser des réseaux sociaux de très grande taille [18].

Sur la base de la référence [18], une catégorisation des axes de recherche dans le domaine des réseaux sociaux en ligne a été proposée. Cette catégorisation comprend dix-sept axes de recherche dont nous citons quelques-uns comme : la détection des individus spéciaux ayant des caractéristiques spéciales, le Commerce et le marketing, le Contrôle et l'analyse des activités des utilisateurs, le Crawling , la recommandation et la suggestion, l'extraction de réseau social , et la privacy qui est un domaine de recherche que les chercheurs ont largement étudié.

7 Modélisation des réseaux sociaux et la théorie des graphes

De nombreux domaines ont aujourd'hui recours aux graphes dans le but de traiter des problèmes rencontrés dans le monde réel. Parmi ces domaines, on trouve notamment ceux traitant les réseaux sociaux. La théorie des graphes est un outil puissant de modélisation conduisant à des solutions efficaces. Elle a été développée depuis le 20ème siècle. Elle a été largement appliquée dans le domaine de la modélisation de réseau social. Les chercheurs ont essayé d'utiliser la théorie des graphes pour analyser quantitativement les réseaux sociaux et ont obtenu des résultats prometteurs. [13]. La section suivante liste quelques notions de la théorie des graphes, adaptés aux réseaux sociaux et qui vont être utilisées dans notre mémoire :

- Un **sommet** (ou en anglais vertex) est l'unité de base d'un réseau, il en représente une ressource. Dans un réseau social on parle d'acteur. Le terme **nœud** est également utilisé pour désigner un sommet [6]. Un acteur ou sommet a certaines caractéristiques (ou informations supplémentaires) qui décrivent ses propriétés connus comme des **attributs** ou **labels** comme le nom, l'adresse, le numéro de sécurité sociale (SSN), numéro de téléphone, etc.
- Une **arête** (edge) est un lien ou une connexion entre deux sommets. On parle également d'arc dans le cas d'un graphe orienté. Les relations sont représentées par des arêtes (les relations peuvent être des connaissances proches, amitié, … etc.). [6]
- Un **graphe** est défini par un ensemble de sommets et un ensemble d'arêtes. C'est le couple G = (V, E), où V est l'ensemble des sommets et E ⊆ V x V l'ensemble des arêtes qui les relient. Le terme de réseau peut être employé en tant que synonyme de graphe dans certaines disciplines telles que la biologie ou la sociologie. Le terme de nœud devient alors synonyme de sommet et le terme de lien synonyme d'arête. Nous notons n = |V| le nombre de sommets, et m = |E| le nombre d'arêtes [12].
- Un graphe G est dit **non dirigé** (ou **non orienté**) si l'ordre des arêtes n'est pas pris en

compte, i.e. pour toute paire (u, v) ∈ E, la paire (v, u) ∈ E. Dans le cas contraire, le graphe est dit **dirigé** (ou **orienté**) ou graphe avec des arêtes orientées ou arcs [12]. Un **graphe simple** est un graphe dans lequel pour toute paire de sommets u et v il n'existe qu'un seul lien (u, v) ∈ E, et dans lequel les auto-boucles ont été retirées : $(v,v) \notin E, \forall v \in V$. Dans le cas contraire, on parle de multi-graphe [12]. Un **graphe étiqueté** est un graphe où chacune des arêtes est affectée soit d'une chaîne de caractères, soit d'un nombre ou d'un symbole. Ces symboles sont appelés étiquettes ou label [7]. Un **graphe pondéré** est un graphe étiqueté auquel on associe une fonction de pondération f(u,v) qui associe un poids à chaque arête (u,v) ∈ E. Le poids des arêtes permet de les hiérarchiser, en s'appuyant par exemple sur des notions de similarité ou de proximité des sommets [12]. Un graphe est **complet,** ou clique si pour toute paire de sommets u, v, il existe au moins une arête (u,v) reliant u et v [12]. Un **graphe simple complet d'ordre n** s'appelle une n-clique [6].

- Le **degré** d'un sommet v noté d(v) est le nombre d'arêtes issues du sommet v dans un graphe non orienté ou le nombre d'arcs arrivant ou partantes du sommet v dans un arc orienté. La distribution des degrés est la proportion p_k, pour chaque entier k, de sommets de degré égal à k dans le graphe G : $p_k = \frac{1}{n} . |v \in V, d(v) = k|$ [12]

- Un **chemin** est une séquence de liens permettant de relier deux sommets entre eux. Une propriété importante caractérisant la structure des réseaux complexes est le plus court chemin entre les nœuds [35]. la longueur d'un chemin représente le nombre de liens (arêtes ou arcs) dans cette séquence. Si les deux sommets sont les mêmes, alors le chemin est un cycle [12]. La longueur faible de plus court chemin moyen par rapport au nombre de nœuds est une propriété caractérisant la plupart des réseaux sociaux. Cette propriété a été d'un intérêt particulier en sociologie et elle est populairement connu comme « l'effet petit monde » ou le concept de « six degrés de séparation », qui suggère que la distance entre deux personnes quelconques dans un réseau social est en moyenne très courte (elle est proche de six ou plus petit dans l'étude expérimentale de Milgram [20]) [35]. Un **chemin orienté** est une séquence d'arêtes qui relie deux sommets en respectant l'orientation du parcours à chaque arête. [6]

- Deux sommets sont dits **connexes** s'il existe au moins un chemin de longueur finie permettant d'aller de l'un à l'autre [12]. Une **composante connexe** est un ensemble maximal de sommets qui sont tous reliés par un même chemin. Un graphe est dit connexe s'il ne contient qu'une composante connexe (il existe un chemin entre toute paire de sommets). [12]

- La **distance** entre deux sommets u et v, notée d(u,v) correspond à la longueur d'un plus court chemin qui relie les deux sommets (il peut y en avoir plusieurs). Si aucun chemin ne permet pas de les relier, la distance est infinie et les deux sommets ne sont pas connexes. [12]

- Le **diamètre** d'un graphe est la plus grande distance qui existe entre deux sommets quelconques du graphe. Comme cette mesure n'a de sens que si le graphe est connexe, on la restreint en pratique en calculant le diamètre de la plus grande composante connexe. Si le graphe est connexe, **la distance moyenne** ou **APL** correspond à la moyenne de la distance entre toutes les paires de sommets. Les notions de distance moyenne et de diamètre capturent le nombre d'intermédiaires à franchir (respectivement en moyenne et au plus) pour aller d'un sommet à un autre dans le graphe [12].

- La **densité**, notée &(G), d'un graphe G qui contient au moins deux sommets correspond au rapport entre le nombre de liens du graphe et le nombre de liens possibles : [12]

$$\&(G) = \frac{|E|}{\binom{n}{2}} = \frac{2|E|}{n(n-1)}$$

- Un **parcours de graphe** permet de visiter les sommets d'un graphe en suivant ses liens. Les parcours les plus couramment utilisés sont le parcours en largeur (breadth-search first, ou BFS) et le parcours en profondeur (depth-search first, ou DFS). Dans les deux cas, on choisit un sommet de départ que l'on appellera la racine et on parcourt ses voisins, les voisins des voisins, et ainsi de suite, tant que l'on rencontre de nouveaux sommets. Les voisins d'un sommet sont appelés ses enfants. Dans un parcours en largeur, on explore d'abord tous les enfants de la racine, puis tous les enfants des enfants, et ainsi de suite. Dans un parcours en profondeur, on explore d'abord un enfant, puis le premier petit enfant, et ainsi de suite, avant de parcourir les enfants suivants. Le parcours en largeur s'implémente facilement avec une file, tandis que le parcours en profondeur s'implémente plutôt avec une pile. [12]

Modéliser une situation à l'aide d'un graphe revient à identifier l'ensemble des sommets (nœuds) et à caractériser l'ensemble des arêtes (arcs). Nous utiliserons la notation suivante pour la suite de document :

- Un graphe est noté G = (V, E) avec V l'ensemble des sommets, E l'ensemble des arêtes, n=|V| est le nombre de sommets et m=|E| est le nombre d'arêtes.
- Un sous graphe de G est noté S = (V_S, E_S) avec $V_S \in V$, $E_S \in E$ et restreint à des arêtes reliant des sommets de V'.
  - v_i désigne le $i^{ème}$ sommet.
  - (v_i, v_j) désigne une arête entre les sommets v_i et v_j.
  - Le degré d'un sommet v_i est noté d(v_i).

Les graphes non orientés sont adaptés pour les réseaux sociaux avec des relations non orientées. Les graphes orientés sont adaptés pour représenter des relations non symétriques comme les réseaux de confiance par exemple. Les graphes pondérés sont adaptés aux réseaux sociaux qui contiennent différents niveaux d'intensités dans les relations. Les graphes étiquetés permettent de représenter différents types de relations [6]. Dans le cadre de notre mémoire, nous parlerons de graphes simples, non-orientés et non pondérés. La figure 1.2 ci-dessous montre une structure d'un simple réseau social avec 7 nœuds représentant des individus et les salaires sont des attributs sensibles montrés par des labels. S'il y a un lien entre deux nœuds, sa indique qu'ils ont communiqué entre eux.

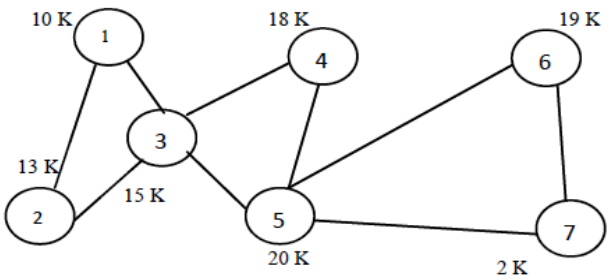


Figure 1.2 : Graphe de réseau social avec 7 nœuds et les salaires comme attributs sensibles

- La matrice est l'objet mathématique le plus utilisé pour manipuler ces concepts, mais des approches ensemblistes ont aussi était proposées. On distingue deux types de matrices dans un réseau social, les matrices d'incidence et les matrices d'adjacence. On parle de matrice d'adjacence lorsqu'on a les mêmes ressources en ligne et en colonne, on obtient ainsi une matrice carrée avec la ligne i et la colonne i représentant la même ressource. Un graphe peut ainsi être représenté sous la forme d'une matrice M à n lignes et n colonnes représentant un tableau. Chaque case de ce tableau est notée a_{ij} avec i et j les numéros respectifs de ligne et de colonne de la case. La valeur contenue dans la case a_{ij} est le poids de la relation entre les ressources v_i et v_j (égal à 1 dans le cas d'un graphe non pondéré), 0 correspond à une absence de relation [23].

Dans notre mémoire, nous utilisons les paires de termes suivantes de façon interchangeable : « réseau » et « graphe », « nœud » et « sommet », « arête » et « lien », « entité » et « individus », « attaquant » et « adversaire ».

8 Les caractéristiques communes des graphes sociaux

Les graphes permettent de modéliser de nombreuses configurations issues du monde réel. Il peut s'agir de réseaux de transport (routes et voies aériennes) et de communication (téléphonie, réseau Internet), mais aussi de réseaux issus du web (graphe du web), de réseaux d'usage (comme les réseaux de Co-citation dans les articles scientifiques , Réseaux de collaboration des acteurs), ou encore de **réseaux sociaux** (relations de contacts) …etc. Ces graphes ne sont pas définis de manière formelle, ce qui les distingue des familles de graphes étudiées en théorie des graphes (comme les graphes aléatoires par exemple). La forte augmentation des données disponibles a permis de réaliser une suite de travaux qui ont abouti à la constatation que ces graphes partagent souvent des propriétés structurelles communes [12].

8.1 La distribution des degrés suit une loi de puissance

Ces graphes se caractérisent en premier lieu par une distribution hétérogène des degrés de leurs sommets. De tels graphes sont appelés des graphes sans échelle (scale-free networks), car il n'existe pas de sommet représentatif, en raison des grandes différences d'ordre de grandeur entre leurs degrés. Plutôt que d'être caractérisée par une moyenne, comme c'est le cas pour une distribution normale, la distribution des degrés est souvent assimilée à une loi de puissance [12]. On dit qu'un réseau présente une distribution des degrés suivant une loi de puissance si le nombre de nœuds de degré k est proportionnel à $1/k^{\alpha}$ pour une constante $\alpha > 0$, sur un intervalle de plusieurs ordres de grandeur (par exemple entre k = 10 et k =10^6) [19], à savoir que plus on considère un degré élevé, plus le nombre de sommets qui ont ce degré dans un même réseau est faible. La figure 1.3 montre la répartition des degrés dans le réseau social du club de karaté de Zachary [6].

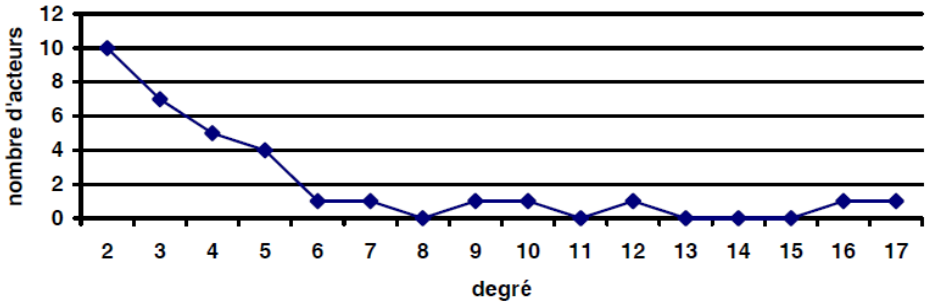


Figure 1.3 : Répartition des degrés du club de karaté de Zachary [6]

8.2 Réseaux petit monde

Une deuxième caractéristique importante de ces graphes est une distance moyenne et un diamètre court. Cette observation, relevée dès 1967 dans le cadre d'une des fameuses expériences du psychosociologue « Stanley Milgram » [20] et confirmée par les mesures de grands réseaux à partir des années 1990, jusque récemment sur le réseau de Facebook, à travers le travail de Backstrom et al en 2012, est souvent résumée sous le concept de « six degrés de séparation », qui sépareraient en moyenne deux personnes choisies au hasard dans la population mondiale [12]. Autrement dit, chacun puisse être relié à n'importe quel autre individu par une courte chaîne de relations sociales, ce qui implique la séparation entre deux personnes quelconques dans le réseau est faible, ainsi dans un réseau social de taille n, le plus court chemin entre deux sommets est de l'ordre de log(n) [6]. Ainsi lorsque la taille du réseau augmente, la longueur des plus courts chemins n'augmente que très peu [6]. En effet, le diamètre est beaucoup plus faible que le nombre de sommets [12]. On parle alors de réseaux petits monde (small world en anglais).

Ce phénomène (appelé aussi effet du petit monde) tient son nom de l'expression populaire « le monde est petit » désignant la surprise de constater que deux connaissances d'un même individu à priori sans rapport, se connaissent entre elles. L'étude des relations sociales en tant que réseau d'interactions date des années 30, en particulier la création par le psychologue Jacob-Levy Moreno de la sociométrie. Celle-ci a pour but la mesure objective des relations sociales au sein d'un groupe [19]. C'est dans une période ultérieure de développement de la science des réseaux sociaux que les psychologues se sont intéressés à l'effet petit monde [20].

L'expérience du « petit monde » [20] consiste à demander à des groupes de personnes (environ 300 personnes) choisies aléatoirement de Nebraska de faire suivre une lettre jusqu'à un agent de change, vivant à une adresse fournie dans Boston. Les participants pouvaient seulement passer les lettres, de main à main, à des connaissances personnelles qu'ils pensaient être capables d'atteindre l'objectif, directement ou via leurs connaissances [20]. Relativement peu de lettres sont arrivées à destination, mais le résultat surprenant fut que la longueur moyenne d'une chaîne de porteurs du message de son origine à sa destination était très faible en regard du nombre d'individus et de leur éloignement géographique et social [19]. Milgram [20] décrit le fait que les lettres arrivées à destination étaient passées par six personnes en moyenne et en conclut que deux citoyens américains pris au hasard sont à une « distance » de six poignées de main l'un de l'autre.

Bien que seulement 5% des lettres soient arrivées à destination, cette expérience est considérée comme le point de départ de l'étude des réseaux petits mondes. Cette étude a été suivie par de nombreuses autres avec divers outils (téléphone, courriers électroniques,…etc.) et des travaux à la frontière entre informatique et sociologie ont vu le jour pour tenter de comprendre l'existence de ces chemins courts [22]. Alors que cette étude avait été faite manuellement, l'avènement de l'informatique et de l'Internet ouvre de nouvelles voies pour l'étude des réseaux sociaux, en offrant une quantité phénoménale de données riches et disponibles instantanément. Parmi ces réseaux, certains reposent sur des applications de l'Internet, comme les réseaux d'échanges de courriers électroniques reliant les personnes qui s'en envoient, alors que d'autres réseaux sont simplement disponibles dans des bases de données, comme le graphe des acteurs dans lequel les acteurs ayant joué dans un même film sont reliés. [22]

La notion de petit monde n'a pas aujourd'hui de définition formelle ; elle est définie, dans certains articles comme la combinaison d'un fort coefficient de clustering et d'un petit diamètre [19], Ils sont caractérisés par une distance courte entre les individus du réseau et par le fait que deux individus qui possèdent un voisin commun ont une forte probabilité d'être adjacents. Il est aujourd'hui admis que bon nombre de réseaux du monde réel sont des réseaux petits monde, parmi eux on trouve :

- Réseaux de réaction chimique,
- Réseaux neuronaux,
- Réseaux biologiques,
- Réseaux de chaîne alimentaire,
- Réseaux de collaboration scientifique,
- Réseaux de citations des papiers scientifiques,
- Réseaux de collaboration des acteurs,
- Réseaux sémantiques ou lexicaux,
- Réseaux sociaux,
- …etc.

8.3 Structure communautaire

Ces graphes se caractérisent également par de fortes densités locales, cela implique que deux sommets ont significativement plus de chances d'être connectés s'ils partagent un voisin en commun. Cette caractéristique joue un rôle essentiel dans la morphologie des grands réseaux, dans la mesure où elle peut conduire à la constitution de zones denses qui peuvent permettre de délimiter les contours de communautés. Ces propriétés permettent essentiellement de les distinguer des graphes aléatoires qui sont étudiés depuis bien plus longtemps [12]. Pour les réseaux sociaux cette caractéristique est issue de la tendance de l'homme à se socialiser en groupe ce qui donne aux réseaux sociaux une forte tendance au clustering (grands coefficients de clustering) et une structure en communautés qui sont par exemple des groupes d'amis, de collègues de travail, de loisirs, de famille, etc. Une définition largement acceptée, liée à la topologie du réseau, considère une communauté comme un sous-graphe dont les sommets sont plus liés entre eux qu'avec d'autres sommets du réseau [5]. Autrement dit, une communauté est un ensemble de sommets dont la densité de connexions internes est plus forte

que la densité de connexions vers l'extérieur [34], ou des groupes de sommets avec une forte densité d'arêtes et reliés entre eux par des ponts. Un exemple d'un réseau avec une structure claire en communautés est illustré dans la figure ci-dessous. Cette socialisation s'effectue avec une tendance à l'affiliation entre des nœuds ayant des propriétés quasi-équivalentes [6].

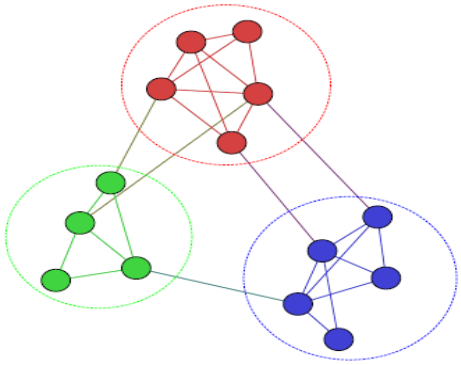


Figure 1.4 – Un exemple de graphe avec trois communautés identifiées [34]

Les sites de réseautage social permettent aux utilisateurs de partager des idées, des images, des messages, des activités, des événements et des intérêts avec les gens dans leur réseau. En raison de ces comportements sociaux en ligne des communautés sont formées, où les utilisateurs en ligne ont tendance à former des communautés qui regroupent les utilisateurs qui partagent quelques intérêts en commun. Les utilisateurs forment généralement des groupes ou des cercles dans le réseau social en ligne. Dans Facebook, un utilisateur peut créer des listes d'amis qui sont du même contexte comme les amis de lycée, les amis de collège, les collègues de travail, la famille, etc. ces listes forment des communautés de personnes avec les même intérêts ou des personnes qui se connaissent forment le même contexte [14].

9 L'Analyse des réseaux sociaux

Avec la croissance rapide des réseaux sociaux et la disponibilité des traces de communication numériques, enregistrées et stockées dans des serveurs centralisés, l'analyse de tels réseaux, a attiré beaucoup d'attention dans le domaine de la recherche. L'analyse des réseaux sociaux a émergé comme une technique clé dans la sociologie moderne, ainsi que dans la science politique, l'ingénierie industrielle, la géographie, l'économie et la science de l'information. Le but de l'analyse de réseau social est de découvrir des modèles sociaux cachés. La puissance de l'analyse de réseau social a été montrée beaucoup plus forte que celle des méthodes traditionnelles qui se concentrent sur l'analyse des attributs des différents acteurs sociaux. Dans l'analyse de réseau social, les relations et les liens entre les acteurs sociaux dans un réseau sont souvent considérés plus important et plus informatif que les attributs des différents acteurs sociaux. [32]

9.1 Historique et Définition

La recherche dans l'analyse des réseaux sociaux a une longue histoire d'environ 100 ans. En 1994, Wasserman et Faust ont défini l'analyse des réseaux sociaux comme: «Social Networks Analysis is a research methodology based on sociology, it can be used to analyze the model between relationship and the interaction between actors" [24]. Plutard, les méthodologies et les mesures d'analyse des réseaux sociaux ont été largement appliquées dans différents domaines, tels que la sociologie, la biologie et la technologie de l'information, etc. Hanneman

et Riddle [28] ont souligné qu'un réseau social est composé par des acteurs, des relations et des liens. L'analyse des réseaux sociaux s'intéresse aux relations entre les acteurs sociaux, ces acteurs pouvant être des individus, des groupes d'individus, des entreprises, etc. [28]. En ce sens, l'analyse des réseaux sociaux se présente comme une boîte à outils comprenant un ensemble de méthodes, de concepts, de théories, de modèles et de techniques, mobilisables dans les différentes disciplines des sciences sociales comme dans d'autres domaines, et qui consistent à prendre pour objets d'étude non pas les différentes propriétés des acteurs étudiés (quand il s'agit d'individus : leur âge, leur sexe, leur niveau de diplôme, leur profession, etc.), mais les relations entre ces acteurs (quelle que soit la nature de ces relations) et les régularités qu'ils présentent[17]. La majorité des méthodes et outils existants sont basés sur des méthodes statistiques et fournissent un grand nombre de fonctionnalités d'analyse et de modélisation. Dans le livre « Social Network Analysis» [23], les concepts de base, les mesures et les méthodologies ont été très bien introduits.

Les approches d'analyse de réseau social ont été montrées très utile en capturant et en expliquant de nombreux phénomènes du monde réel comme le phénomène bien connu « petit monde » [32].

9.2 Types d'analyse des réseaux sociaux

L'analyse des réseaux sociaux est l'un des domaines de recherche émergents pour extraire des informations utiles à partir des données de ces réseaux. Comme déjà présenté dans la section 2, un réseau social est composé d'un ensemble d'acteurs sociaux et des relations d'interaction entre ces acteurs. Généralement, il y a trois types de tâches d'analyse ou de vues prises dans les études sur les réseaux sociaux comme le montre la figure ci-dessous : la vue orientée structure, la vue orientée acteurs, et la vue orientée structure-acteurs. [26]

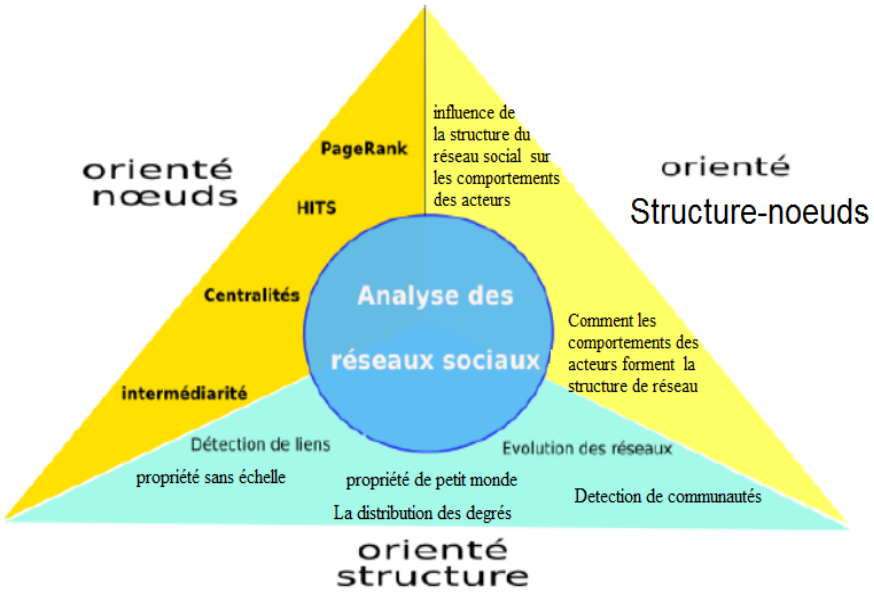


Figure 1.5: Analyse de réseaux sociaux : les vues ou les tâches (image inspirée de [5])

a) Dans la vue orientée structure, les chercheurs se concentrent seulement sur l'analyse des caractéristiques structurelles du réseau entre les acteurs sociaux, telle que la propriété de la distribution aléatoire des degrés, la propriété sans échelle, la propriété de petit monde, ou la propriété de la structure en communautés [20]. Dans cette vue, les acteurs sociaux sont abstraits dans des nœuds uniformes dans les graphes, et leurs caractéristiques de comportement sont négligés.

b) Dans la vue orientée acteurs, les chercheurs se concentrent principalement sur l'analyse des caractéristiques et des effets de comportements des acteurs sociaux dans les réseaux sociaux (le rôle ou la position d'un nœud dans le réseau [5]). Cette caractérisation va permettre d'obtenir plusieurs informations sur les nœuds (trier les nœuds selon leurs caractéristiques, inférer l'importance d'un acteur dans un réseau, etc.) [5]. Dans ce type de vue, les caractéristiques des structures topologiques des réseaux sociaux ne sont pas considérées [26].

c) Dans la vue orientée acteur-structure, les acteurs sociaux et la structure de réseau sont les deux des sujets de préoccupation. Dans ce type de vue, les chercheurs étudient à la fois comment la structure du réseau social influent les comportements des acteurs et comment les comportements des acteurs forment la structure du réseau [26].

9.3 Applications de l'analyse des réseaux sociaux

L'analyse des réseaux sociaux a plusieurs applications : [74]

- Étude de la structure des réseaux permet de détecter les communautés.
- Utilisation dans le web pour la recherche et l'extraction d'information.
- Utilisation dans le marketing pour identifier des groupes de clients ou produits pour faire des recommandations (publicité ciblée, marketing virtuel).
- Étudier le fonctionnement des réseaux informatiques et de comportement émergent des systèmes physiques et biologiques.
- Étudier la transmission d'une maladie dans les communautés, et suivre l'évolution des épidémies.
- Détection de collusions et de fraudes.
- Sécurité (détection des cellules de terrorisme).

10 La sécurité dans les réseaux sociaux en ligne

Un réseau social en ligne comme déjà définit dans la section 3 est une plateforme ou un type de site web qui permet de développer des réseaux sociaux virtuels entre des personnes ayant en commun des intérêts, des activités, et des contextes. Ces réseaux permettent aux utilisateurs de trouver de nouveaux amis et de développer leurs cercles d'amis. Le partage est une des caractéristiques importantes de ces réseaux. Les utilisateurs partagent des données personnelles sur les réseaux sociaux sans être entièrement conscients des conséquences, ils peuvent partager leurs photos, vidéos, activités, intérêts et beaucoup plus de sujets qui varient en fonction des principaux objectifs du réseau. La grande quantité d'informations que les utilisateurs partagent sur ces réseaux sans tenir compte du facteur de sécurité rend ces réseaux

une cible souhaitable pour les hackers et peut conduire l'utilisateur à devenir une victime d'une attaque de sécurité.

Pour résoudre les problèmes de sécurité dans les réseaux sociaux, chaque site de réseautage social en ligne a une certaine politique de respect de la vie privée qui permet aux membres de contrôler l'accès à leurs informations personnelles, par exemple, les utilisateurs de Facebook peuvent contrôler qui pourra les trouver par l'outil de recherche par mot-clé de Facebook, et quelles informations peuvent être vues quand ils les trouvent. En outre, les utilisateurs de MySpace peuvent spécifier les utilisateurs autorisés à les voir quand ils sont en ligne, et ils peuvent bloquer l'accès à leurs profils par âge ou par identité. De plus, de nombreux sites permettent aux utilisateurs de contrôler quelles mises à jour de leur compte sont visibles et par qui, spécifier des limites différentes pour les différentes parties de leurs informations, par exemple une personne peut décider que ses photos sont visible seulement par ses amis proches. Cependant, les attaquants auraient certainement essayé de passer ces frontières.

Dans cette section, nous allons étudier les différents types de menaces de sécurité dans les réseaux sociaux en ligne ainsi que le problème du respect de la vie privée de ses utilisateurs. Nous citons aussi quelques solutions existantes pour atténuer ces risques.

10.1 Menaces de sécurité dans les réseaux sociaux

Au fur et à mesure que la popularité des sites de réseautage social augmente chaque jour, ainsi que la grande quantité d'informations personnelles partagées, les menaces de sécurité dans ces réseaux et la possibilité d'exposition aux risques de fuite d'informations augmentent également. Les pirates informatiques, les spammeurs, les auteurs de virus, les voleurs d'identité et d'autres criminels suivent le trafic. À ce titre ces réseaux sont vulnérables à plusieurs menaces de sécurité qui exploitent soit les données personnelles d'un utilisateur ou les vulnérabilités des réseaux sociaux. L'étude dans [29] décrit quinze risques de sécurité, auxquels les utilisateurs ou les fournisseurs de SNSs peuvent faire face, tels que:

10.1.1 L'ingénierie sociale « Social engineering »

Les utilisateurs des réseaux sociaux en ligne parfois sans le savoir partagent des informations personnelles avec des inconnus. Par exemple, les numéros de téléphone, l'adresse e-mail personnelle et professionnelle, les images et les informations de localisation de l'utilisateur qui sont facilement disponibles. Toutes ces informations pourraient être utiles quand elles sont combinées avec des techniques d'ingénierie sociale où les attaquants emploient les vulnérabilités humaines pour lancer des attaques d'ingénierie sociale. Pour cela, ils essaient de tromper l'utilisateur, que c'est une action légitime [41]. Parmi les techniques d'ingénierie sociale utilisée nous trouvons « ***Le phishing »,*** c'est une technique utilisée par les pirates dans le but d'obtenir des informations privées et sensibles de l'utilisateur tel que le mot de passe, numéro de carte de crédit, date de naissance, etc. Elle consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance authentique telle qu'une banque, une administration, etc. [31]

Dans ce type d'attaque, l'attaquant tente de cloner un site web légitime d'une manière que la fausse copie semble pratiquement identique à l'original. La figure 1.6 montre un exemple d'attaque de phishing lancée en falsifiant la page de connexion de Twitter. Dans cet exemple, le faux URL qui est très similaire à l'URL légitime de Twitter est repéré par un carré rouge.

Dans la majorité des cas, la victime ne fait pas assez d'attention à l'URL dans la barre d'adresse. [30]

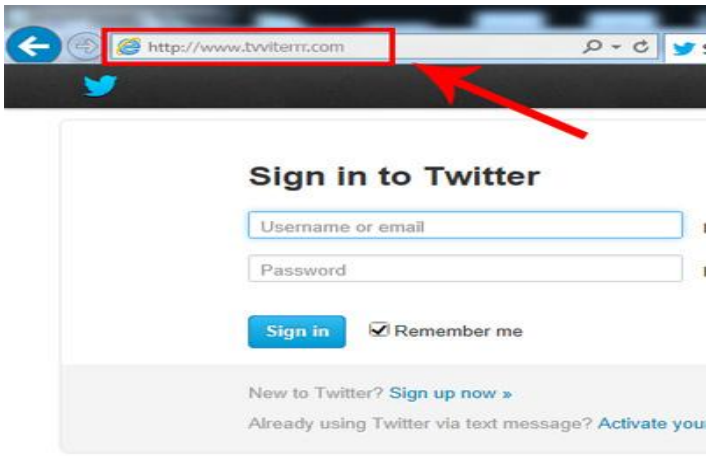


Figure 1.6 : Un exemple d'une attaque de Phishing en falsifiant la page de connexion de Twitter

Dans les réseaux sociaux, pour le lancement de l'attaque de phishing l'attaquant a besoin d'amener la victime à la page falsifiée. Pour diriger les utilisateurs aux pages de phishing, les attaquants utilisent différentes techniques tels que le partage de l'URL de cette page avec un titre attirant ou une image dans le réseau social.

Il est considéré que, les personnes qui utilisent les sites de réseaux sociaux sont plus probables d'être affectées par les attaques de phishing en raison de la nature inhérente de la confiance. En outre, il a été observé que les attaques de phishing augmentent chaque jour. Selon le rapport du renseignement de sécurité Microsoft, environ 85% des attaques de phishing ont ciblé les individus utilisant les réseaux de médias sociaux [31].

10.1.2 URLs raccourcies malveillants "Malicious Shortened URLs"

Les services de « shortener URL » sont conçus pour rendre la mémorisation des longues URL possible en raccourcissant leur longueur en quelques lettres (URL très court, qui Cache la véritable URL de destination, difficile de dire où vous allez jusqu'à ce que vous cliquez). Exemple de ces services est Goo.gl et bit.ly. Dans les réseaux sociaux les attaquants utilisent ces services pour l'obscurcissement des URL malveillants. Par exemple, un lien vers un site web malveillant peut s'afficher sur le fil d'actualités de l'ami de la victime. Les attaquants utilisent les services de raccourcissement d'URL « URL shortener services » pour cacher l'adresse de l'URL malveillant.

Une autre façon d'encourager l'utilisateur à cliquer sur le lien raccourci malveillant est par l'ingénierie sociale. Un exemple de cette technique : l'attaquant envoie un message à une victime avec ce contenu "Hey cette personne *bit.ly/yyyy* répand des rumeurs horribles sur vous ...» Ce message soulèvera la curiosité de la victime pour vérifier l'URL et lire les rumeurs. Cependant cet URL raccourcie pointe vers un site web malveillant qui peut infecter son ordinateur. [30]

10.1.3 Les logiciels malveillants « Malwares »

Un logiciel malveillant ou *Malware* peut être n'importe quelle application malveillante conçue pour interrompre des opérations informatiques, pour récolter les données d'un utilisateur et / ou accéder directement à ses informations personnelles. Les *Malware*s peuvent également utiliser les infrastructures des réseaux sociaux pour se propager entre les différents utilisateurs dans le réseau, infectant l'ordinateur d'un utilisateur et s'étendre ensuite à ses contacts. C'est parce que le malware peut sembler provenir d'un contact de confiance, et donc les utilisateurs sont plus susceptibles de cliquer sur les liens et / ou télécharger des programmes malveillants. Le premier logiciel malveillant semblable était "Koobface", qui avait les propriétés de se propager sur le réseau social pour acquérir le login et le mot de passe, et de transformer la machine en botnet [31].

Certaines techniques courantes utilisées dans la propagation de malwares incluent : [38]

- Les URL raccourcies, en particulier sur les réseaux de mise à jour de statut ou fils d'actualité. Ceux-ci peuvent conduire l'utilisateur à télécharger un virus ou visiter un site qui va tenter de charger des malwares sur l'ordinateur d'un utilisateur.
- Les messages qui semblent provenir de contacts de confiance qui encouragent un utilisateur à cliquer sur un lien, voir une vidéo ou télécharger un fichier.
- Un e-mail semblant provenir du réseau social lui-même, pour demander des informations ou demander à l'utilisateur de cliquer sur un lien.
- Les applications tierces qui infectent les ordinateurs avec des logiciels malveillants et se propagent aux contacts.

10.1.4 Applications tierces malicieuse « Malicious Third Party Applications »

Certains réseaux sociaux en ligne tels que Facebook et Twitter peuvent permettre à l'utilisateur d'utiliser des applications tierces. Dans le contexte des réseaux sociaux, "les applications tierces" sont des programmes qui interagissent avec un réseau social sans être nécessairement partie de ce réseau [38]. Ces applications fournissent plus de fonctionnalités supplémentaires pour le réseau social [41]. Ces fonctionnalités prennent de nombreuses formes : jeux en ligne, sondage ou quiz en ligne, applications de communication, rencontres et beaucoup d'autres formes.

Pour rendre ces applications utiles, les réseaux sociaux peuvent permettre aux développeurs un accès automatique aux informations publiques des utilisateurs. Par exemple dans Facebook; la photo du profil, le nom, le genre, et le pseudo ou le nom d'utilisateur sont des informations publiques et elles sont également disponibles pour ces applications [39]. De plus, les privilèges des applications ne sont pas limités à cela, ils peuvent également accéder à une certaine partie d'informations personnelles ou privés du profil d'utilisateur. Un utilisateur peut accorder un accès aux applications tierces à son profil sans se rendre compte des permissions étendues étant accordées. Dans certains cas, elles peuvent avoir l'accès à toutes les images de l'utilisateur, la liste d'amis, les messages ainsi que le fil d'actualités (le mur). Cependant, Ces applications pourraient être malveillantes intentionnellement ou elles pourraient être vulnérables et exploitées par des attaquants.

Les applications intentionnellement malveillantes peuvent se propager en postant de fausses publicités d'elles-mêmes sur le mur de la victime pour attirer plus d'utilisateurs. Par exemple, dans Facebook une application annonce qu'elle peut fournir des informations sur les noms des visiteurs du profil. Une fois la victime va à l'application et lui permet de commencer à

travailler, l'application commencera à se partager sur le fil d'actualités de la victime avec la même technique. Il existe différents types de techniques de propagation utilisées par ces applications malveillantes telles que le partage sur le fil d'actualités, le partage dans les messages, et le marquage des amis sur l'image de l'application [30].

Dans certains cas, l'application est légitime mais elle pourrait être vulnérable et plus tard exploitée par un attaquant. Ensuite l'attaquant peut avoir toutes les privilèges que l'application avait sur ses utilisateurs. Les problèmes de sécurité qui pourraient exister dans les applications tierces citons les plus communes dans les applications web, comme le *Cross Site Scripting (XSS, Les failles d'injection),* les injections SQL, … etc. [30].

10.1.5 Usurpation ou vol d'identité « Identity Theft »

Partager des informations personnelles sur les réseaux sociaux peut mener au vol d'identité. Ces informations peuvent permettre aux attaquants de récolter assez d'informations pour voler l'identité de la victime [30]. En 2009, des chercheurs de l'université « Carnegie Mellon » ont publié une étude montrant qu'il est possible de prévoir la plus grande partie des chiffres et parfois tous les neuf chiffres du numéro de sécurité sociale d'un individu en utilisant les informations tirées des réseaux sociaux et les bases de données en ligne [38].

Les informations souvent ciblées par les voleurs d'identité incluent :

- Les mots de passe
- Les informations de compte bancaire
- Les numéros de carte de crédit
- Les informations stockées sur l'ordinateur d'un utilisateur comme les contacts
- Les numéros de sécurité sociale.

Même quelques détails personnels simples peuvent fournir suffisamment d'informations à l'attaquant pour deviner des mots de passe, répondre aux questions de récupération de mot de passe ou plus [41]. Par exemple les pages que l'utilisateur aime dans Facebook reflètent ses intérêts, ces intérêts affinent pour l'attaquant les possibilités de deviner le mot de passe en faisant quelques combinaisons entre la date de naissance publique de la victime et ses intérêts pour deviner le mot de passe.

Une autre technique utilisée consiste à se faire passer pour l'identité de quelqu'un pour tromper une victime et apparaître comme quelqu'un qu'il connaît bien et donc lui convaincre d'établir un lien. Principalement pour obtenir l'accès au système informatique ou aux données confidentielles. Cette technique peut être combinée avec d'autres techniques par les pirates. Par exemple aimer la page d'une banque dans Facebook. En aimant la page d'une banque X, la victime fournit l'information qu'elle a éventuellement un compte dans cette banque. L'attaquant utilise cette information pour concevoir une attaque Phishing avec la page de connexion du site web de la banque et l'envoyer à l'e-mail de la victime dans le but de voler ses informations d'identification bancaires [30].

Dans un autre cas toutes les informations publiques récoltées sur les utilisateurs telles que le nom, le pays, la ville, la date de naissance, et la photo sont stockées dans des bases de données et plus tard se vendront à des criminels pour créer des faux documents physiques tels que les passeports et les cartes d'identité [30].

10.1.6 Les Spams

Les spams c'est un autre problème de sécurité dans les réseaux sociaux en ligne. Ce sont des messages envoyés en grande quantité aux internautes, il s'agit en général à des fins publicitaires. Les spammeurs établissent généralement les liens sociaux avec des milliers d'utilisateurs, puis tentent de diffuser du spams sur les liens sociaux. Les spams dans les réseaux sociaux semblent être plus réussis comparant aux spams traditionnels qui utilisent les emails pour la diffusion. Et cela est dû à la relation sociale entre les utilisateurs qui apportera plus de confiance. Faire confiance aux amis peut facilement convaincre la victime de lire le message de spam, et de croire à son contenu [30]. Le Spam devient un sérieux problème quand il est combiné à la diffusion de codes malveillants (malwares). Grier et al dans [33] ont analysé 25 millions d'URLS partagés sur Twitter et ont découvert que 8% d'entre eux pointent vers des pages web répertoriées dans des listes noires comme elles contiennent des codes malveillants. L'utilisateur, en cliquant sur une URL avec un code malveillant, infecte son ordinateur et permet au propriétaire de malware d'accéder à son compte. En analysant les comptes utilisés pour l'envoi de spams, les auteurs ont également trouvé des preuves que les massages de spams ont été lancés par des comptes légitimes infectés par un code malveillant.

10.1.7 Les faux utilisateurs "Fake Users"

Les réseaux sociaux en ligne essayent de faciliter la procédure d'inscription des utilisateurs pour attirer plus d'utilisateurs. Par exemple, par le processus simple qui demande seulement un nom, une adresse email et un mot de passe. Cette procédure encourage les utilisateurs à s'inscrire plus facilement. Cependant, elle facilite également le processus de création de faux comptes. Par exemple, Facebook a publié une statistique qui révèle environ 83 millions de ses utilisateurs sont des faux utilisateurs. Un faux utilisateur reste sans danger pour les utilisateurs légitimes à moins qu'il ne soit connecté avec eux. Dans ce type d'attaque, l'attaquant crée un faux compte avec des informations d'apparence légitimes comme un faux nom, ville, date de naissance. Ensuite, il tente de devenir ami avec la victime. En acceptant une demande d'amitié d'un faux compte la victime exposera ses informations personnelles à l'attaquant. [30]

Toute personne sur un réseau social peut créer un compte ou une page sous le nom d'une marque, une société en toute illégalité. Il revient aux organisations de vérifier les comptes existants sous leur nom et d'en demander la fermeture si elles considèrent que cela nuit à leur image. La fondation « Abbé Pierre » déclare par exemple devoir gérer la fermeture de faux comptes sur Facebook. [10]

10.1.8 Redirection d'apparence légitime « Legitimate Look Redirect »

La plupart des réseaux sociaux en ligne ont une page spécifique pour rediriger l'utilisateur vers une autre destination. La destination peut être à l'intérieur du réseau social ou un autre site. Habituellement ce système est utilisé pour faire des statistiques de référencement à cette adresse de destination. Cependant les attaquants utilisent ce système pour rediriger l'utilisateur vers une URL malveillante. Par exemple l'adresse suivante montre un exemple d'un tel service dans Facebook : https://www.facebook.com/l/e9bf8;www.maliciouswebsiteaddress.com

Cette technique est utilisée pour cacher l'URL malicieux des yeux de la victime. L'adresse malveillante existe toujours à la fin de l'URL, mais elle attirera moins d'attention. De nos jours, la plupart des réseaux sociaux tels que Facebook, informent l'utilisateur par une alerte avant de quitter Facebook vers une nouvelle destination. Cette alerte indique un message

concernant cela «vous allez quitter le site Facebook à un autre site web nommé : XYZ, Êtes-vous sûr que vous voulez le faire". Ce type d'avertissement atténue le risque de cette attaque. Néanmoins encore certains utilisateurs poursuivent et vont à la destination malveillante. [30]

10.2 Quelques solutions existantes

Bien que les Malwares, le phishing et même les attaques XSS aient été traités dans le passé, elles continuent de se propager largement en raison de la constitution des médias sociaux. Il existe différentes solutions pour atténuer les menaces de sécurité dans ces réseaux. Ces solutions peuvent varier de techniques offertes par les opérateurs de réseaux sociaux à des conseils de sensibilisation à la sécurité. La combinaison de ces solutions peut améliorer le niveau de sécurité de l'utilisateur dans l'environnement cyber : [30]

10.2.1 Outils de sécurité d'URL

Différentes entreprises de logiciels commencent à produire des petits outils comme des modules ou extensions sur les navigateurs pour vérifier la sécurité des URLs. Ces outils par l'accès à la base de données en ligne des attaques de phishing et des sites web malveillants peuvent déterminer si l'URL cible en fait partie ou non. Généralement, ces bases de données sont fournies par de célèbres éditeurs de logiciels antivirus ou des sites web anti-phishing. Par exemple « Bitdefender » actuellement a publié une extension nommée "Traffic Light" qui vérifie tous les liens à l'intérieur du Facebook et Twitter et s'assure de leur sécurité. Dans le cas où ils sont malveillants une croix rouge apparaît à côté du lien, dans le cas contraire un signe de contrôle vert indique que le site est propre. Cette solution peut atténuer efficacement le risque de phishing, des URLs malveillants, des redirections d'aspects légitimes et des liens de spam.

10.2.2 Ajuster les paramètres de confidentialité

Actuellement, la plupart des sites de réseaux sociaux ont placé l'entière responsabilité de la confidentialité des données à l'utilisateur seul en lui fournissant une large gamme d'options de réglage des paramètres de confidentialité configurables qui permettent aux utilisateurs de restreindre la visibilité de certains contenus sur leurs profils. Néanmoins, de nombreux utilisateurs naïfs conservent les paramètres de confidentialité par défaut, ce qui rend tous leurs détails publiquement visible. En se référant à la section de la vie privée du réseau social il faut réajuster ces paramètres. L'utilisateur doit s'assurer qui sont capable de voir son/ses albums de photos, vidéos, messages, commentaires, liste d'amis, statut de relation et d'autres détails des informations personnelles. Il est suggéré fortement de minimiser le niveau de partage public. Cette solution permettra d'atténuer le risque de vol d'identité et des spams.

10.2.3 Ajuster le niveau d'accès des applications

En se référant aux paramètres de la vie privée il faut s'assurer qu'il n'y a pas d'applications installées à l'insu de l'utilisateur. L'utilisateur peut également vérifier les privilèges de chaque application et s'il voit une simple application qui demande des privilèges élevés plus que nécessaire, ça peut être un cas suspect et c'est recommandé de ne pas permettre de donner ces privilèges à cette application. Autre chose, l'utilisateur doit veiller à enlever les anciennes applications qu'il ne les utilise plus. Cette solution permettra d'atténuer le risque d'applications tierces malveillantes.

10.2.4 Partage limité

La plupart des réseaux sociaux permettent à l'utilisateur de catégoriser ses amis. Après avoir accepté toute invitation d'ami, Il est suggéré de veiller à les mettre dans la bonne catégorie. Et au moment du partage il devrait s'assurer de choisir le bon groupe et ne pas partager toutes les informations avec tous les amis. Par exemple, un utilisateur peut avoir deux groupes « famille » et « camarades de classe ». Au moment de partage des photos de famille, il doit limiter l'accès à la catégorie « famille ». Également, il est recommandé fortement de ne pas partager de l'information personnelle et privée publiquement. Cette solution permettra d'atténuer le risque de phishing, de spams, de vols d'identité et de faux utilisateurs.

10.2.5 Réfléchir à deux fois

Avant d'effectuer n'importe quelle action dans les environnements de réseaux sociaux, il faut bien réfléchir. Lorsque l'utilisateur veut accepter une nouvelle demande d'ajout d'ami, il devrait s'assurer s'il connaît cette personne dans le monde réel. Il est recommandé vivement d'éviter d'accepter les demandes d'ajout des personnes inconnues, à la réception de telles demandes c'est conseillé de refuser la demande ou si c'est nécessaire faire un coup d'œil sur le profil du demandeur pour décider de l'accepter ou non. Autre chose, comme discuté précédemment, les attaques de phishing sont très fréquentes, par conséquent, tous les liens reçus dans un courriel ou dans une discussion avec des amis en ligne doivent être considérés avec prudence et ne doivent pas être cliqués à moins que réputés fiables et authentiques. Cette solution permettra d'atténuer le risque de faux utilisateur, phishing, spams et de vol d'identité.

La table 1.1 ci-dessous récapitule l'efficacité de chaque solution contre les différentes menaces dans les réseaux sociaux en ligne :

Solutions / Menaces	Outils de sécurité d'URL	Ajuster les paramètres de confidentialité	Ajuster le niveau d'accès des applications	Partage limité	Réfléchir à deux fois
Phishing	√			√	√
URL malicieux	√				
Vol d'identité		√		√	√
applications tierces malveillantes			√		
Spams	√	√		√	√
Faux utilisateurs				√	√
Redirections Ligitimes	√				

Table 1.1 : Résumé des menaces et solutions.

11 Conclusion

Les réseaux sociaux en ligne peuvent être un service efficace et amusant pour les utilisateurs pour partager leurs intérêts et s'engager avec des amis sans limitations géographiques et économiques. En même temps, ces réseaux peuvent mettre l'utilisateur face aux risques importants de sécurité. Le nombre important des utilisateurs de ces réseaux a attiré l'attention des attaquants. La bonne compréhension des problèmes de sécurité dans les réseaux sociaux peut aider l'utilisateur à apprendre, comment mieux atténuer les risques de sécurité.

Ce chapitre nous a permis de faire un état de l'art sur le concept des réseaux sociaux ainsi que les menaces de sécurité dans ces réseaux, nous avons discuté comment chacune de ces menaces pourrait mettre l'utilisateur en danger.

Une autre préoccupation commune liée à la sécurité dans les réseaux sociaux concerne la vie privée et plus précisément, la protection des informations sensibles et privées qui est devenue de plus en plus un problème sérieux quand les données du réseau social sont publiées pour un usage public**.**

Avant les réseaux sociaux, les problèmes concernant la préservation de la vie privée lors de la publication des bases de données [27] a été largement étudiée. C'est un domaine qui tente de répondre au problème de la façon dont une organisation, comme un hôpital, une agence gouvernementale, ou une société d'assurance, peut libérer des données au public sans violation de la confidentialité des informations personnelles. Le développement des techniques de traitement des données tout en préservant la vie privée est devenue une direction fructueuse pour la recherche dans les bases de données et le data mining. L'objectif principal de la recherche est comment cacher les informations sensibles tout en publiant les données pour un usage public. (Par exemple, dans le domaine de la santé publique, les données médicales qui incluent les relations familiales des individus sont maintenant disponibles pour des fins de l'analyse des données).

Au-delà des bases de données, les risques de divulgation de la vie privée sur les réseaux sociaux se posent quand le propriétaire des données veut publier ou partager les données de réseau social avec une autre partie pour la recherche. Ce problème sera abordé dans le prochain chapitre, ainsi que les solutions prévues pour garantir le respect de la vie privée des utilisateurs de ces réseaux.

1 Introduction

L'avènement des réseaux sociaux au cours des dernières années a créé une énorme quantité de données du réseau social qui pourraient être potentiellement utilisées pour plusieurs fins. Ainsi, ceci peut être d’une grande importance d’obtenir des informations utiles à partir des données de réseaux sociaux, tels que le comportement de l'utilisateur, la croissance de la communauté, la propagation d’une maladie, etc. Ces données doivent être publiées dans certaines situations, notamment quand le propriétaire des données doit partager les données avec des tiers tels que des partenaires publicitaires qui font partie des politiques généralement acceptées par les souscripteurs. Ces données contiennent des informations précieuses sur les utilisateurs qui aident les partenaires publicitaires d’améliorer le ciblage des publicités, Par exemple, Facebook mentionne explicitement dans sa politique de confidentialité que les profils des utilisateurs peuvent être partagés pour des fins de publicités personnalisées tout en prétendant anonymiser ces données. Les réseaux sociaux ont été utilisés comme objet d'étude dans de nombreux domaines tels que la sociologie, l'épidémiologie, le marketing, la psychologie, l'économie et les sciences de l'information. Donc, les données doivent être partagées ou publiées dans toutes les situations mentionnées ci-dessus. Cependant, il est primordial que les données publiées ne doivent pas révéler des informations privées sur les individus. La vie privée est une des préoccupations majeures lors de la publication ou de partage des données des réseaux sociaux pour la recherche ou autre buts d’analyses. Par conséquent, le challenge est comment protéger la vie privée des individus et en même temps préserver l'utilité des données du réseau social.

Les données d'un réseau social peuvent être représentées sous forme d’un graphe social, où les sommets représentent les individus et les arêtes représentent les relations entre les individus. En plus de sommets et d'arêtes, des informations supplémentaires sur les individus et leurs relations peuvent être représentées par des étiquettes ou labels. Les labels de sommets peuvent représenter les attributs d'une personne, comme l'identité, le genre, et la localisation. Les labels d’une arête peuvent représenter les attributs sur les relations, y compris la nature des relations, par exemple, l'amitié, la parenté, et co-auteur, ainsi que le poids de relations qui peut décrire par exemple le degré d'une amitié.

Puisque les données du réseau social ont souvent des informations privées sur des individus ainsi que sur leurs relations sensibles, le partage de ces données dans leur forme brute peut violer la vie privée des individus. Par conséquent, préserver la vie privée tout en publiant les données du réseau social devient un des problèmes principaux pour les utilisateurs du réseau et un domaine de recherche très important. Des travaux ont été réalisés par divers chercheurs dans ce sens.

Jusqu'à présent, nous avons seulement considéré les graphes sociaux représentant les réseaux sociaux en ligne. En fait, les graphes sociaux ont été également utilisés pour représenter des données provenant de nombreuses sources hors ligne incluant les bases de données des hôpitaux, les opérateurs téléphoniques et d'autres organismes gouvernementaux. Les attaques sur les réseaux sociaux utilisent souvent le graphe social publié pour violer la vie privée. Dans ce chapitre, il y a plusieurs questions clés à aborder, à savoir le compromis entre la vie privée des utilisateurs et le partage des informations d’utilisateur en public, les attaques sur le graphe publié qui ont pour but la violation de la vie privée des individus du réseau social, les approches d’anonymisation proposées dans la littérature, la perte de l'information lors de l’anonymisation du graphe du réseau social, etc.

2 La publication des données de réseaux sociaux

Aujourd'hui, de plus en plus les données des réseaux sociaux ont été publiées d'une manière ou d'une autre à des tiers, tels que les développeurs d'applications, les chercheurs, les sociologues et les sociétés commerciales. Ces données sont très précieuses pour ces tiers, puisqu'ils peuvent analyser ces données pour extraire les informations dont ils ont besoin pour leurs objectifs particuliers. Par exemple, une entreprise peut utiliser les données qui forment la base de profils des clients, pour promouvoir ses produits à ces clients à travers un système de recommandation en ligne et peut même utiliser les liens entre les utilisateurs du réseau social pour élargir leurs bases de clients [71]. Les employeurs peuvent également utiliser les réseaux sociaux pour identifier des clients potentiels ou recruter des employés candidats. Par exemple, selon les statistiques publiées dans Time Magazine en 2007, 12% des employeurs aux États-Unis utilisaient déjà les sites de réseautage social populaires tels que MySpace et Facebook pour étudier les profils de certains employés potentiels [32]. Les sociologues peuvent analyser ces données pour mieux comprendre l'évolution des communautés sociales dans le monde physique [71]. Ces tiers obtiennent habituellement ces données soit par l'analyse d'un site de réseau social « crawling » via l'interface publique fournie par le propriétaire d'OSN ou en demandant ces données au propriétaire d'OSN qui publie régulièrement les données d'OSN. [71].

Cependant, comme ces publications contiennent des informations privées et personnelles en plus de ce qui est disponible publiquement sur le réseau, celles-ci peuvent être ciblées par des attaques de ré-identification, où un attaquant tente de récupérer les identités des nœuds qui ont été déjà supprimées et la vie privée sera violée si ces données étaient publiées directement. [71] Par exemple l'entreprise « Enron », l'une des plus grandes entreprises américaines, qui a déclaré faillite en 2001 a publié 500.000 e-mails qui sont analysés par les chercheurs. Cet ensemble de données a grandement facilité la recherche sur la correspondance par courriel, la structure organisationnelle, et l'analyse de réseau social, mais il a aussi probablement entraîné des violations substantielles de la vie privée pour les individus impliqués [101]. Par conséquent, la préservation de la vie privée lors de la publication des données de réseau social est devenue une préoccupation très importante.

L'objectif de l'administrateur de données « data trustee » qui les recueillent est de publier une version des données qui permet une analyse utile tout en préservant la vie privée des entités représentées. C'est un domaine qui tente de répondre au problème de la façon dont l'administrateur de données peut publier les données du réseau social sans violation de la confidentialité des informations privées. Cela se fait typiquement par l'anonymisation, qui traite un réseau social comme un graphe et lui applique diverses transformations pour atteindre la sécurité.

Comme déjà mentionné dans le chapitre 1, les données de réseau social peuvent être représentées sous forme de graphe non orienté, dans lequel les sommets correspondent généralement à des individus ou d'autres entités sociales, et les arêtes correspondent aux liens sociaux entre eux [24]. Chaque entité peut avoir un certain nombre d'attributs, tels que l'âge, le genre, le revenu et un identifiant unique. Toujours, comme première étape de l'anonymisation pour préparer les données de réseau social à la publication tout en préservant les propriétés globales du réseau, est de supprimer les attributs identifiants les nœuds tels que le nom ou le numéro de sécurité sociale. Afin de préserver les identités des nœuds dans le graphe, des identifiants synthétiques aléatoires sans signification sont introduits pour

remplacer les noms des entités sociales. Cette procédure est appelé « l'anonymisation naïve » d'un réseau social [62].

L'anonymisation naïve est une pratique courante qui répond aux objectifs d'utilité, car la plupart des analyses de réseau social peuvent être effectuées en l'absence des identificateurs d'entité (telles que le nom ou le numéro de sécurité sociale). Ainsi la motivation derrière l'anonymisation est comme suit: Puisque le réseau social étiqueté par les vrais noms est « sensible » et ne peut pas être publié, il peut y avoir une valeur considérable en permettant aux chercheurs d'étudier sa structure. Pour telles études, les chercheurs ne sont pas particulièrement intéressés par "qui" correspond à chaque nœud, mais par les propriétés du graphe, comme la connectivité, les distances nœud-à-nœud, les fréquences de petits sous-graphes, etc. L'anonymisation vise donc à préserver la structure du graphe tout en supprimant l'information «qui». Autrement dit, le but de l'anonymisation est de:

- Fournir des données réelles utiles pour des études sans compromettre la vie privée des utilisateurs du réseau social.
- Permettre aux tiers de tester de nouvelles techniques d'analyse et de data mining sans penser aux propriétaires des données.

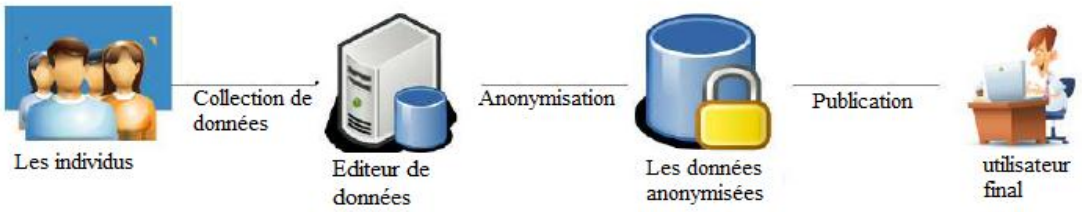


Figure 2.1 : Collection et publication de données

Préserver la vie privée lors de la publication de données peut être représenté sous forme de phases comme le montre la figure 2.1 ci-dessus, la phase de « collecte de données » et la phase de « publication de données ». En phase de collecte, les données réelles sont rassemblées auprès des propriétaires par l'éditeur de données « data publisher » qui est un serveur de confiance. L'éditeur de données à son tour modifie les données en les anonymisant d'une manière qui garantit la confidentialité des informations personnelles, ensuite dans la phase de publication il les publie au destinataire des données qui peut être des data-miner et peut également être des adversaires.

Plusieurs formulations du problème de protection des données publiées des réseaux sociaux sont possibles dans trois dimensions importantes: les informations privées, les connaissances de base de l'adversaire, et l'utilité des données [32]. Dans la section 4, nous classons l'information dans les réseaux sociaux, et nous modélisons la vie privée, les connaissances de base de l'adversaire et par ailleurs, nous étudions l'utilité des réseaux sociaux, qui est le but principal d'optimisation de l'anonymisation.

3 La « vie privée » ou la « privacy » dans les réseaux sociaux

La vie privée a été un sujet de discussion bien avant l'avènement des réseaux informatiques. Cependant, la notion de vie privée a pris un tour dramatique dû à la prolifération des outils et applications de la technologie de l'information, qui est encore aggravée par les sites de réseautage social qui permettent aux utilisateurs de montrer leurs informations de profil pour

être vues et partagées par des millions de visiteurs en ligne. Cela donne le potentiel de l'utilisation négative de leurs informations. Certaines données du réseau social peuvent être privées et doivent être protégées contre toute divulgation non autorisée.

Le concept de la vie privée a souvent généré une certaine controverse quand les chercheurs ont essayé de le définir différemment et dans des perspectives différentes. Dans [91], la vie privée est considérée comme : « the right of the individual to decide what information about himself should be communicated to others and under what circumstances » ou « le droit de l'individu de décider quelles informations le concernant devraient être communiquées aux autres et dans quelles circonstances », autrement dit une violation de la vie privée se produit quand des informations privées et confidentielles sur l'utilisateur sont révélées à un adversaire. Lijie Zhang et al [51] ont considéré une donnée personnelle est privée si elle est prévue par son propriétaire d'être cachée de la consultation publique, où son propriétaire peut être la personne décrite par les données ou l'organisation qui détient les données. La vie privée alors de ce qui précède pourrait être considérée comme un sujet relatif.

Dans un réseau social en ligne, une donnée peut être désignée privée par un membre ou par une politique de l'ensemble du système. En général, s'il faut désigner une donnée privée est une décision personnelle et peut varier d'une personne à autre. Peu importe ce qui est désigné privé, la vie privée de la personne est violée si un adversaire obtient avec 100% de certitude une information qui devait être cachée sur la personne [51]. Notons que non seulement les informations liées à un sommet peuvent être privées, mais l'existence d'une arête peut également être privé.

Avec le nombre important d'utilisateurs de réseau social, c'est compliqué de tracer le concept de la vie privée. La vie privée est un sujet qui a reçu beaucoup d'attention et a différents aspects. Cependant, sur les réseaux sociaux en ligne certaines caractéristiques principales qui sont à la base de la vie privée sont généralement identifiées. Parmi ces concepts l'anonymat « *anonymity* », l'intraçabilité « *unlinkability* » et la non observabilité « *unobservability* » sont les plus intéressants pour protéger la vie privée. Premièrement, l'anonymat garantit qu'un attaquant ne peut pas identifier suffisamment un utilisateur au sein d'un ensemble d'utilisateurs, Autrement dit, l'impossibilité de déterminer la véritable identité de cet utilisateur. Deuxièmement, l'intraçabilité se réfère à l'incapacité d'un attaquant de distinguer entre différentes opérations réalisées par un même utilisateur. Troisièmement, la non-observabilité protège l'activité d'un utilisateur afin qu'un attaquant ou un tiers ne puisse pas dire si une ressource ou un service est utilisé c.-à-d. un utilisateur peut utiliser une ressource ou un service sans que d'autres utilisateurs ou observateurs soient capables de déterminer si une action est en cours. Aujourd'hui, ce sont les préoccupations de la vie privée des utilisateurs les plus courantes. [49]

4 Modélisation de la préservation de la vie privée dans les réseaux sociaux

Pour lutter contre les attaques de la vie privée et développer des techniques de protection, selon Bin Zhou et al [32] nous devons tout d'abord modéliser trois aspects. Premièrement, nous devons identifier les informations privées qui peuvent être l'objet d'attaques. Deuxièmement, nous devons modéliser les connaissances de base que l'adversaire peut utiliser pour attaquer la vie privée des individus cibles. Enfin, nous devons spécifier l'usage des données publiées du réseau social anonymisé afin qu'une méthode d'anonymisation puisse maintenir l'utilité autant que possible alors que les informations privées sont entièrement préservées.

4.1 Les informations personnelles ou privées dans les réseaux sociaux

Dans la préservation de la vie privée dans les bases de données relationnelles, les attributs dans une table sont divisés en deux groupes: les attributs non sensibles et les attributs sensibles. Les valeurs des attributs sensibles sont considérées privées pour les individus. Néanmoins, dans les données de réseaux sociaux, beaucoup plus d'éléments d'information peuvent être considérés comme information privée pour les individus. Par définition, les données sensibles dans le contexte de réseau social se réfèrent aux attributs d'utilisateurs dans les profils des nœuds qui sont considérés comme privées et ont un accès contrôlé. En outre, certaines relations entre des nœuds peuvent être des données sensibles [93]. Liu et al. [60] et Zheleva et Getoor [61] ont proposé un schéma de catégorisation des informations privées. Ils ont classifié la violation de la vie privée dans les réseaux sociaux en 3 catégories :

a. ***La divulgation d'identité*** **:** c'est-à-dire, l'identité d'un individu (exemple : nom, numéro de sécurité social, adresse email ...) qui est associé à un nœud est révélée. Ce type de violation conduit à la révélation des informations de l'utilisateur et des relations qu'il partage avec d'autres personnes dans le réseau.
b. ***La divulgation de lien sensible***: c'est-à-dire, la relation sensible entre deux individus est révélée, et
c. ***La divulgation du contenu ou d'attribut sensible***: La divulgation d'attribut sensible se produit quand un attaquant obtient des informations d'un attribut sensible et confidentiel d'un utilisateur. Les attributs sensibles peuvent être liés avec une entité et une relation sensible, par exemple, les messages électroniques envoyés et/ou reçus par les individus dans un réseau de communication par email.

En outre, Zhou et Pei [32] ont proposé une autre classification plus étendue des informations privées qui englobe :

- ***Existence de sommet :*** Dans les données du réseau social, si un individu cible apparaît ou pas dans le réseau peut être considéré comme information privée pour l'individu. Par exemple, supposons un réseau social de millionnaires est publié où chaque sommet dans le réseau représente un millionnaire. S'il peut être déterminé qu'un individu cible apparait dans le réseau, un attaquant sait que la cible est un millionnaire. Comme autre exemple, un réseau d'infection d'une maladie est très utile dans la recherche pour la santé publique. Néanmoins, si un adversaire détermine qu'un individu cible apparaît dans le réseau, alors l'information privée d'avoir l'infection est violée.

- ***Propriétés de sommet*** : Dans les données du réseau social, certaines propriétés d'un sommet comme le degré peuvent être considérés comme information privée pour l'individu. Par exemple, si un adversaire connaît le degré d'un individu cible dans un réseau de soutien financier, l'adversaire sait combien de sources de soutien que la cible possède.

- ***Labels sensibles de sommet :*** Dans les données du réseau social, les sommets peuvent porter des attributs représentés sous forme de labels, qui peuvent être divisés en deux catégories: labels non sensibles et labels sensibles. Comme dans le cas des données relationnelles, les valeurs des labels sensibles de sommets sont considérées comme information privée pour les individus. Par exemple, dans un réseau d'infection de maladie, chaque individu peut être associé avec un label sensible de maladie. La maladie d'un individu cible peut être identifiée par des adversaires une fois la cible peut être lié d'une

manière unique à un sommet dans le graphe ou à un groupe de sommets ayant le même label sensible dans le graphe.

- ***Labels sensibles d'arête :*** Dans les données du réseau social, les arêtes peuvent aussi porter plusieurs labels. Comme dans le cas ci-dessus des labels de sommets, les labels d'arête peuvent être divisés en labels non sensibles et labels sensibles. Les valeurs des labels sensibles d'arête sont considérées comme information privée pour les deux individus correspondants.

- ***Existence de relation ou de lien :*** Dans les données du réseau social, une arête entre deux sommets indique qu'il existe une relation entre les deux individus correspondants. Le lien entre les sommets peut être considéré comme information privée pour les individus. Par exemple, dans un réseau de transactions financières, deux sommets sont reliés par une arête s'il y a une transaction financière qui se passe entre eux. Un adversaire peut détecter si deux individus ciblés ont des transactions financières si une arête entre ces individus existante dans un tel réseau peut être déterminée.

- ***Poids du lien :*** Certains réseaux sociaux peuvent être pondérés. Les poids des arêtes peuvent refléter l'affinité entre deux sommets ou enregistrent le coût de la communication entre deux individus. Par exemple, un réseau social de communication entre amis peut être pondéré de telle sorte que le poids d'une arête est la fréquence de communication entre deux individus, qui peut être considérée comme information privée pour certaines personnes.

- ***Métriques de graphe:*** Dans l'analyse de réseau social, de nombreuses métriques de graphe ont été proposées pour analyser la structure de graphe, telles que le betweenness ou l'intermédiarité (c.à.d., le degré d'un individu de se trouver entre d'autres individus dans le réseau directement ou indirectement), le closeness ou la proximité (c.à.d., le degré d'un individu d'être proche à d'autres individus dans le réseau directement ou indirectement), la centralité (qui compte le nombre de relations avec d'autres individus dans le réseau), la longueur de chemin (c.à.d., les distances entre les paires de sommets dans le réseau), l'accessibilité (c.à.d., le degré pour un membre quelconque du réseau de pouvoir atteindre d'autres membres du réseau), et ainsi de suite. Toutes ces métriques peuvent être considérées comme information privée pour certains individus.

La modélisation des informations privées est importante qui permet de mettre en place l'objectif de la préservation de la vie privée dans les réseaux sociaux. Différentes préoccupations liées à la vie privée peuvent conduire à différentes définitions du problème et en conséquence à différentes méthodes de sa préservation.

4.2 Les connaissances de base de l'adversaire

L'une des difficultés les plus importantes dans la publication des données est l'information auxiliaire (aussi appelée connaissances externes ou connaissances de base) qu'un adversaire peut récolter d'autres sources d'informations tels que le web ou les enregistrements publiques. Par définition, une connaissance représente toute sorte d'information sur les utilisateurs du réseau social que possède l'adversaire et qui n'est pas nécessairement directement liée au réseau social, mais qui peut être obtenue à travers plusieurs moyens et qui peut servir pendant l'attaque par inférence [72]. Une attaque par inférence sur un graphe social anonymisé a pour but de causer une violation de la vie privée des individus en divulguant certaines informations

personnelles non présentes explicitement dans le graphe social rendu public. Comme par exemple, son affiliation politique ou sa relation avec une autre personne.

Sur les données relationnelles, une grande catégorie d'attaques à la vie privée est de ré-identifier les individus en rejoignant la table publié avec certaines tables externes modélisant les connaissances auxiliaire des adversaires. Plus précisément, les adversaires sont supposés connaître les valeurs des attributs quasi-identifiant des victimes cibles. Pour les réseaux sociaux, en raison des structures complexes de données du graphe, les connaissances de base des adversaires peuvent être modélisées de différentes façons. Dans [32], Zhou et al ont énuméré plusieurs types de connaissances de base: les attributs de sommets, les relations de lien spécifiques entre certains individus cibles, les degrés de sommets, les voisinages de certains individus cibles, sous-graphes incorporés, et les métriques de graphe qui seront détaillées dans ce qui suit : [32]

• ***Identifier les attributs des sommets :*** Un sommet peut être lié uniquement à un individu par un ensemble d'attributs, où l'ensemble d'attributs jouent un rôle similaire à un quasi-identifiant dans les attaques de ré-identification sur les données relationnelles. Les attributs du sommet sont souvent modélisés comme des labels dans un graphe social. Un adversaire peut connaître quelques valeurs d'attributs de certaines victimes, par exemple, l'adversaire peut savoir que l'âge de Bob est 18 ans, et il habite en France. De telles connaissances peuvent être utilisées pour lier Bob à des sommets dans le réseau.

• ***Degré de sommet :*** Le degré d'un sommet dans le réseau capture le nombre d'arêtes qui le relient aux autres sommets. Une telle information est souvent facile à recueillir par les adversaires. Par exemple, le voisin d'un individu cible peut facilement estimer le nombre des amis de la victime. Un adversaire qui a la connaissance de degré de la victime peut ré-identifier l'individu cible dans le réseau en examinant les degrés des sommets dans le réseau anonymisé publié.

• ***Existence de relation ou de lien :*** Un adversaire peut savoir qu'il y a des liens spécifiques entre certains individus cibles. Par exemple, dans un réseau social d'amitié, les arêtes peuvent porter des labels enregistrant l'utilisation des personnes des canaux pour communiquer entre eux, tels que le téléphone, l'email et/ou la messagerie. Un adversaire peut essayer d'utiliser la connaissance qu' : « une victime utilise seulement des e-mails pour contacter ses amis dans le réseau » pour lier la victime à des sommets dans le réseau.

• ***Voisinages*** (***Neighborhoods) :*** Un adversaire peut avoir la connaissance de base sur le voisinage de certains individus cibles. Par exemple, un adversaire peut savoir que la victime a quatre amis proches qui se connaissent. En utilisant cette connaissance de base, l'adversaire peut ré-identifier la victime en recherchant les sommets dans le graphe social dont les voisinages contiennent une clique de taille au moins 4. Généralement, nous pouvons considérer le *d*-voisin d'un sommet cible, c.-à-d., les sommets sur une distance *d* du sommet cible dans le réseau, où *d* est un nombre entier positif.

• ***Sous-graphes incorporés*** (***Embedded subgraphs) :*** Un adversaire peut incorporer des sous-graphes spécifiques dans un réseau social avant que le réseau soit publié. Après avoir rassemblé le réseau publié, il est possible que l'adversaire ré-identifie le sous-graphe incorporé si le sous-graphe est unique. Comme montré dans [47], la création de 7 sommets par un attaquant peut révéler une moyenne de 70 sommets cibles.

Tel que mentionné dans [94] pour les graphes simples dans lesquels les nœuds ne sont pas associés avec des attributs et les liens ne sont pas étiquetés, les adversaires ont seulement des connaissances de base structurelles dans leurs attaques (degrés de sommets, voisinages, sous-graphes incorporés, etc.). Par exemple, Liu et Terzi [53] ont considéré les degrés de sommets comme connaissance de base des adversaires pour violer la vie privée des personnes cibles, les auteurs de [54,64] ont utilisé l'information structurelle « voisinage » de certains individus cibles, les auteurs de [47] ont proposé l'utilisation de sous-graphes incorporés.
Pour les graphes riches [94] dans lesquels les nœuds sont associés à divers attributs et les liens peuvent avoir différents types de relations, il est impératif d'étudier l'impact sur la divulgation des informations personnelles lorsque les adversaires combinent les attributs et l'information structurelle dans leurs attaques. Les auteurs, dans [61, 65, 68] ont étudié des techniques d'anonymisation pour différents types de graphes riches contre les connaissances de base complexes.

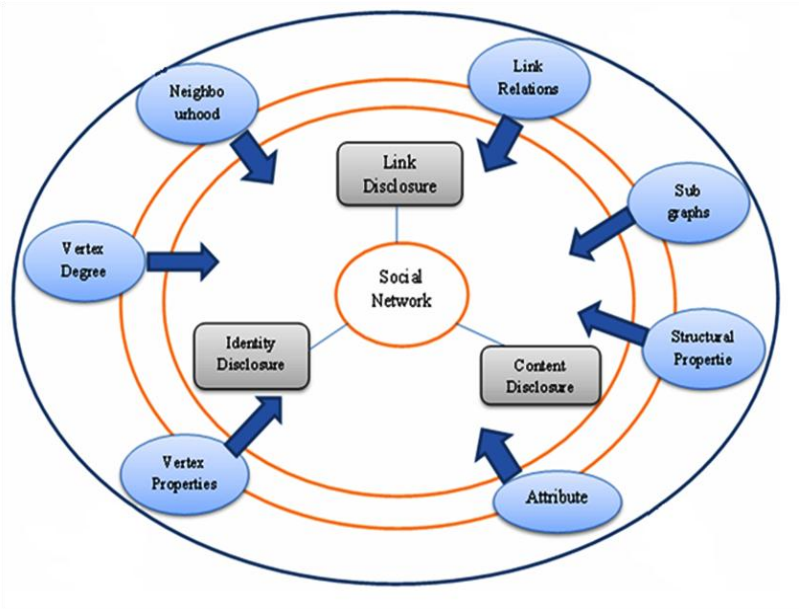


Figure 2.2: La divulgation de la vie privée et les connaissances de base dans les réseaux sociaux [40]

Comme souligné dans les deux Survey [32] et [60], il est très difficile de modéliser tous les types de connaissances de base des adversaires et de quantifier leur impact sur la violation de la vie privée dans le scénario de la publication des données du réseau social. Ci-dessus dans la figure 2.2 un schéma modélisant les connaissances de l'adversaire ainsi que les trois catégories de violation de la vie privée.

- **Quelques sources de connaissances de l'adversaire**

Une partie considérable des attaques sur les réseaux sociaux s'appuie sur le graphe social publié et sur des connaissances auxiliaires que l'adversaire peut acquérir et exploiter. Ces connaissances peuvent être disponibles à travers une source publique au-delà du contrôle du propriétaire de données ou peuvent être obtenus par des actions malveillantes de l'adversaire, par exemple :

- Les sociologistes, épidémiologistes et professionnels de la santé collectent des données correspondantes à différents types de graphes sociaux (famille, liens sociaux et localisations) pour étudier les risques de la propagation de maladies[18]. Il est possible que l'adversaire puisse accéder à ces données suite à une publication d'informations.

- Pour les réseaux sociaux en ligne, les données peuvent être collectées par crawling via une API ou par screen-scrapping. Par exemple, Mislove et al [95] ont collecté les données de réseaux sociaux tels que Flickr, YouTube, LiveJournal et Orkut en utilisant ces méthodes. Les liens d'un utilisateur, avec son profil, sont visibles à ceux qui visitent le compte de l'utilisateur. Ainsi, les utilisateurs sont capables d'explorer le réseau social en suivant les liens d'utilisateur à utilisateur, parcourant les informations de profil et tout contenu contribué des utilisateurs visités. Certains sites, tels que LinkedIn, ne permettent à un utilisateur que de parcourir les autres comptes d'utilisateurs au sein de son voisinage (c.à.d. un utilisateur ne peut pas voir d'autres utilisateurs qui sont dans les deux sauts dans le réseau social); d'autres sites, permettent aux utilisateurs de visualiser n'importe quel autre compte d'utilisateur dans le système [95]. En outre, un adversaire peut obtenir les propriétés de graphe d'une victime en participant activement à un site de réseau social [47].

- Les opérateurs des réseaux sociaux en ligne partagent parfois leurs graphes sociaux avec des opérateurs publicitaires pour leur permettre un meilleur ciblage de la publicité [37]. Par exemple, Facebook mentionne explicitement dans la politique de confidentialité que les profils des utilisateurs peuvent être partagés pour des fins de publicités personnalisées tout en prétendant anonymiser ces données.

- Des applications tierces peuvent être installées sur certains réseaux sociaux et servir à collecter des informations sur les utilisateurs de ces systèmes. Ainsi, l'application Top-Friends qui donne une note de proximité aux amis, développée par la société Slide, a été suspendue car elle ne respecte pas les choix définis par l'utilisateur en termes de protection de ses données sur Facebook[19].

- Les graphes sociaux des appels téléphoniques peuvent être utilisés pour détecter des activités illicites telles que des fraudes et pour détecter des problèmes de sécurité nationale. Ces graphes sociaux contiennent des millions de nœuds.

4.3 L'utilité dans les réseaux sociaux

Un objectif important derrière la publication des données du réseau social est de permettre des tâches d'analyse utiles. Par définition, l'utilité d'un graphe social quantifie à quel point les données issues d'un graphe social (y'compris sa structure topologique) sont utilisables dans l'analyse des réseaux sociaux. Différentes applications peuvent utiliser les données anonymisées de différentes manières. Dans certaines situations, les réseaux anonymisés peuvent être utilisés pour analyser les structures du réseau global. Dans d'autres situations, les réseaux anonymisés peuvent être utilisés pour analyser les microstructures [32]. Formellement, les différentes attentes d'utilisation peuvent conduire à différents schémas

[18] The National Longitudinal Study of Adolescent Health. http://www.cpc.unc.edu/projects/addhealth, 2008.

[19] Facebook. Facebook's privacy policy. http ://www.new.facebook.com/policy.php, 2012.

d'anonymisation. Jusqu'à présent, trois types d'utilité ont été considérés par les analystes d'un graphe social [94] :

- ***Propriétés topologiques ou structurelles de graphe***

L'une des applications les plus importantes de données de réseau social est d'analyser les propriétés de son graphe. Pour comprendre et utiliser les informations dans un réseau, les chercheurs ont développé diverses mesures pour indiquer la structure et les caractéristiques du réseau de différents points de vue. Cela inclut des propriétés telles que : la distribution des degrés des sommets, le diamètre, le coefficient de clustering, etc. Certaines propriétés sont abordées dans [48, 62, 55, 35, 54].

- ***Propriétés spectrales du graphe***

Le spectre d'un graphe est généralement défini comme l'ensemble des valeurs propres de la matrice d'adjacence du graphe ou d'autres matrices dérivées. Le spectre du graphe a des relations étroites avec beaucoup de caractéristiques du graphe et peut fournir des mesures globales pour certaines propriétés du réseau [94]. Des propriétés spectrales sont adoptées pour préserver l'utilité des graphes aléatoires dans [55,35].

- ***Requêtes d'agrégation d'un réseau***

Une requête d'agrégation sur un réseau calcule l'agrégat sur certains chemins ou sous-graphes satisfaisant certaines conditions d'une requête. À titre d'exemple, la requête pourrait être « Quelle est la distance moyenne d'un sommet médecin à un sommet enseignant dans un réseau social ? ». Les requêtes d'agrégation sur un réseau sont utiles dans de nombreuses applications, comme la gestion de la relation client. Dans [65, 68, 54, 63] les auteurs ont considéré l'exactitude de répondre à des requêtes d'agrégation de réseau comme mesure de préservation de l'utilité, c.à.d. si les données publiées du réseau social peuvent répondre à plusieurs types de requêtes avec une grande précision, alors l'utilité des données publiées est élevée.

Les algorithmes préservant la vie privée modifient généralement les ensembles de données par la généralisation et/ou la suppression des valeurs d'origine. C'est évident de voir que plus les données sont subit des changements, moins utile cela devient pour l'analyse de données pour les chercheurs [89]. En général, c'est difficile de quantifier la perte d'information dans l'anonymisation des réseaux sociaux. Pour les données tabulaires, puisque les tuples sont indépendants, la perte d'information dans une table anonymisée peut être mesurée tuple par tuple. La somme de la perte d'information dans les différents tuples constitue la perte d'information au niveau de la table. Cependant, un réseau social est constitué d'un ensemble de sommets et d'arêtes, ainsi la perte d'information ne dépend pas seulement de la perte associée à la modification d'attributs des nœuds mais également la modification de structure de graphe doit être prise en compte [94]. Dans [54] par exemple, Zhou et al ont utilisé le nombre d'arêtes ajoutées entre le graphe original et celui publié pour évaluer la perte d'information structurelle (la perte d'information est représentée comme le coût d'anonymisation). La raison de l'utilisation du coût d'anonymisation pour mesurer la perte de l'information, est qu'un coût d'anonymisation faible indique que des petits changements ont été apportés au graphe original.

La perte de l'information résultant de l'opération d'anonymisation peut être mesurée par combien l'ensemble de données généralisé se rapproche de l'ensemble de données original. Moins il y'a de perte d'informations, meilleure est la qualité des données obtenue après anonymisation. Ceci dépend des différents types d'algorithmes de préservation de la vie privée [89].

Les expériences montrent qu'il y a une corrélation inverse entre la préservation des propriétés du réseau social et la protection de la vie privée de leurs utilisateurs. Plus les informations du réseau sont préservées, plus la protection de la vie privée est faible.

5 Technique de base de protection de la privacy : l'*anonymisation naïve*

Comme déjà mentionné, les données des réseaux sociaux sont devenues une ressource précieuse dans plusieurs disciplines allant de la sociologie, la psychologie, l'économie à l'informatique et l'ingénierie. Ces données aident la communauté des chercheurs à comprendre le comportement des utilisateurs, construire des modèles basés sur les modèles observés, évaluer la propagation de l'information et même de prévoir des événements futurs, par exemple, qui sont probable de devenir des amis sur un réseau social. Cependant, la publication de ces données représente un sérieux problème car elle conduit à la divulgation d'informations personnelles sensibles des utilisateurs de ces réseaux.

Dans le premier chapitre, nous avons discuté de la protection de la vie privée au moyen de limitation d'accès aux informations personnelles des utilisateurs. Dans cette section nous allons décrire une technique utilisée en même temps pour publier les données et protéger la vie privée des utilisateurs appelée « l'anonymisation » qui traite un réseau social comme un graphe.

Formellement, un réseau social est modélisé sous forme de graphe non orienté non étiqueté $G = (V_G, E_G)$, avec *n* sommets $V_G = \{v_1..., v_n\}$ qui correspondent aux individus et m arêtes $E_G = \{(v_i, v_j) | v_i, v_j \in V_G, i \neq j, 1 \leq j \leq n\}$ qui correspondent aux liens sociaux entre eux [24].

Une définition informelle de l'anonymisation dans le contexte de la protection de la vie privée est de remplacer les informations dont la révélation peut nuire à la vie privée des utilisateurs (nom, email, adresse, etc.) avec d'autres données non significatives [18]. L'idée derrière cette approche est qu'il n'est pas possible de porter atteinte à la vie privée d'un utilisateur tant que l'utilisateur reste non identifiable. Par conséquent, l'objectif de l'anonymisation est de prévenir la ré-identification des utilisateurs du réseau social dans le graphe publié. La façon la plus simple et la plus directe d'anonymisation de graphe social est de remplacer les informations d'identification des utilisateurs avec des identifiants aléatoires uniques. Cette technique est appelée *l'anonymisation naïve* [62].

Formellement, l'anonymisation naïve d'un graphe G = (V, E) consiste à produire un graphe isomorphe $G_{na} = (V_{na}, E_{na})$, défini par une bijection aléatoire $f : V \rightarrow V_{na}$. Les arêtes de G_{na} sont $E_{na} = \{(f(x), f(x')) | (x, x') \in E\}$. Par exemple, la figure 2.3 montre un petit réseau social représenté comme un graphe avec son anonymisation naïve, dans laquelle des identifiants synthétiques ont remplacé les noms. La table de correspondance d'anonymisation « anonymization mapping », est montrée à droite, est une table de correspondance aléatoire qui doit être confidentielle [62].

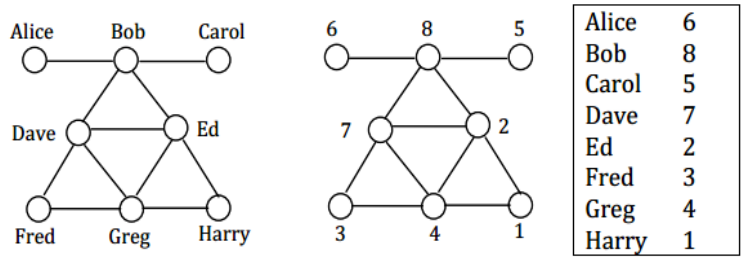


Figure 2.3 : un réseau social représenté comme un graphe (à gauche), l'anonymisation naïve (au centre) et la table confidentielle de correspondance (à droite)

L'administrateur de données tente de cacher G en publiant à sa place un graphe naïvement anonymisé, dans lequel les nœuds de G sont renommés et la structure du graphe n'est pas modifiée.

Notons que cette façon plutôt simple d'anonymisation, n'est pas une garantie d'anonymat contre un adversaire qui se sert d'informations externes sur le réseau social en les combinant avec la structure du graphe publié pour compromettre la vie privée, dé-anonymiser les nœuds, et apprendre l'existence des relations sensibles entre les individus dé-anonymisés [47,60].

6 Les attaques sur les réseaux sociaux naïvement anonymisés

Malgré les efforts fournis pour la protection des informations privées des utilisateurs lors de la publication des données du réseau social utilisant l'anonymisation naïve, ces informations sont toujours exposées à un type particulier d'attaques visant à découvrir des informations dans le graphe anonymisé. Les adversaires peuvent utiliser quelques connaissances de base pour accomplir ce type d'attaques. Par exemple l'attaquant peut avoir des informations spécifiques sur sa cible, et être en mesure de reconnaître sa cible parmi les informations anonymisées. [18]

Comme déjà présenté dans la section 4.1 trois types de violation de la vie privée des individus présents dans un graphe social : (1) la divulgation d'identité, (2) la divulgation de lien et (3) la divulgation d'attribut ou de contenu [60,61]. Ces trois dimensions couvrent toutes les attaques qui pourraient être accomplies sur les données de réseau social publié [34].

Dans notre travail, nous nous concentrons sur la divulgation d'identité où l'objectif de l'adversaire est de ré-identifier une personne déjà connue dans le graphe naïvement anonymisé. Dans la section 6.1 nous allons présenter et détailler les types d'attaques qui ont pour but la divulgation d'identité en décrivant les techniques permettant de faire réussir de telles attaques, et nous donnons un aperçu sur le problème de la divulgation de lien ainsi que la divulgation de contenu dans les sections 6.2 et 6.3 respectivement.

6.1 La divulgation d'identité

Le problème de divulgation de l'identité se pose souvent dans le scénario où le propriétaire des données veut publier ou partager, avec un tiers, un réseau qui permet une analyse utile, sans divulguer les identités réelles des individus impliqués dans le réseau. Ici, chaque individu est représenté par un nœud sur le réseau. Une approche directe pour cacher l'identité de l'utilisateur, est l'anonymisation naïve, en supprimant les informations d'identification personnelles associées à chaque nœud ou en les remplaçant par un nom pseudo-aléatoire ou

pseudonyme avant de publier les données du réseau social dans le but d'éviter que l'adversaire trace avec succès les utilisateurs par leurs véritables identifiants. Il est intéressant de noter que la divulgation de l'identité d'un utilisateur conduit souvent à la divulgation de lien [60].

Backstrom et al. [47] étaient les premiers qui ont proposé des attaques sur les réseaux sociaux naïvement anonymisés, montrant que l'anonymisation naïve n'est pas suffisante pour assurer la vie privée, ainsi si un attaquant a certaines connaissances sur la victime il pourra compromettre sa vie privée. Ils ont identifié une famille d'attaques montrant que même à partir d'une seule copie anonymisée d'un réseau social cachant les attributs d'identification, il est possible pour un adversaire de savoir si des arêtes existent ou non entre certaines paires de sommets spécifiques ciblées. Deux types d'attaques différentes sont présentés dans [47] : les attaques actives et les attaques passives.

Dans le premier type d'attaques, les attaquants affectent le réseau avant son anonymisation et sa publication et peuvent potentiellement construire des sous-graphes fortement distinguables en insérant des nœuds et des arêtes dans le réseau. Cependant, ces attaques sont difficiles à adapter sur une grande échelle car : [58]

- Elles sont limitées aux réseaux sociaux en ligne (OSNs). Créant des milliers de faux nœuds dans un réseau d'appel téléphonique ou un réseau réel est très coûteux ou impossible.
- L'attaquant a peu de contrôle sur les arcs entrant vers les nœuds qu'il a créé. Puisque la plupart des utilisateurs légitimes n'auront aucune raison de faire un lien vers les faux nœuds (appelés aussi les nœuds Sybil), un sous-graphe sans arêtes entrantes mais de nombreuses arêtes sortantes se distinguera. En effet, les attaques actives sont faciles à détecter.
- De nombreux opérateurs de réseaux sociaux comme Facebook ont besoin de faire un lien mutuel avant que l'information est mise à disposition sous toute forme. Par conséquent, en supposant que les utilisateurs réels n'ont pas un lien de retour vers les faux utilisateurs, les liens à partir de faux nœuds vers les vrais nœuds ne se présentent pas dans le graphe du réseau.

« Les attaques passives » quant à elles, sont perpétrés après que le réseau anonymisé soit publié et sans insérer de nouveaux nœuds ou d'arêtes et l'adversaire s'appuie seulement sur l'analyse de données pour inférer des informations privées des utilisateurs.
L'attaque passive est basée sur l'observation que la plupart des nœuds dans un réseau social réel appartiennent à un petit sous-graphe uniquement identifiable. Il est ainsi relativement facile pour un adversaire d'acquérir la connaissance de base du sous-graphe associé à un sommet pour conduire une attaque. Si un adversaire est capable de s'entendre avec d'autres amis dans le réseau, constituant ainsi une coalition notée H, après la publication du graphe il sera en mesure d'identifier et de compromettre la vie privée des voisins connectés à cette coalition. Ils essayent de se retrouver dans le graphe en utilisant la connaissance de la structure du réseau autour d'eux, et de cela ils pourront identifier les voisins connectés à la coalition H et ainsi inférer l'existence de liens entre ces nœuds. Cette implémentation d'attaque ne cible pas un ensemble de nœuds particulier, mais plutôt un ensemble de voisins de la coalition.
Un autre type d'attaques passives différent des attaques proposées dans [47] est présenté dans [51], où l'adversaire utilise également certaines connaissances de base sur les utilisateurs du réseau social pour les identifier et révéler leurs informations privées, en localisant le sommet de la victime et en observant les informations associées à ce sommet. Selon les informations

associées avec les sommets dans le graphe social, Lijie Zhang et al [51] ont classifié les attaques sur le sommet en deux types: la ré-identification de sommet et la réassociation de l'information.

6.1.1 Attaques de ré-identification de sommet

Une exigence simple pour cacher l'information privée dans un graphe de réseau social est de supprimer les identités personnelles, de sorte que le lien entre les personnes et leurs sommets soit caché. Néanmoins, cette solution naïve ne protège pas suffisamment la vie privée contre une attaque de ré-identification de sommet dans laquelle un adversaire utilise quelques connaissances sur la personne cible afin de déterminer le sommet qui la représente [47, 48, 54]. Deux types de connaissances de base ont été utilisés dans les attaques de ré-identification de sommet: attributs de sommet et propriétés topologiques de graphe.

L'utilisation des attributs de sommet pour ré-identifier le sommet d'une victime est similaire à trouver le tuple d'une victime dans une table relationnelle publiée [87], où les labels des sommets sont vus comme des tuples dans une table de données. Certains attributs de la table, comme l'âge, le genre ou le code postal, peuvent être utilisés pour identifier des individus et sont appelés quasi-identifiants (QI). D'autres attributs de la table, comme la maladie ou le salaire, sont considérés comme attributs sensibles. Bien qu'aucune identité personnelle ne figure dans la table, un adversaire peut encore ré-identifier une victime dans la table publiée en utilisant les quasi-identifiants en les associant avec d'autre tables externes, et par la suite dévoiler les valeurs des attributs sensibles.
Wondracek et al [52] ont décrit une attaque utilisant l'appartenance à un groupe dans un réseau social (comme un QI) pour ré-identifier le sommet d'une victime. Un membre d'un groupe peut appartenir à des groupes publics différents dans le réseau social. L'adversaire peut obtenir l'ensemble de ces groupes en piratant l'historique de navigation de la victime par une attaque de sécurité vers le navigateur web de la victime. Cette information peut être utilisée pour construire une empreinte de la victime. De la même manière, à chaque sommet est associée une empreinte. En comparant l'empreinte de la victime avec les empreintes des sommets, le sommet de la victime est ré-identifié, et d'autres informations à propos de la victime peuvent être révélées.

Les propriétés topologiques ou structurelles des graphes est un autre type de connaissances utilisées souvent dans l'attaque de ré-identification de sommet, tels que, le degré de sommet [53], le voisinage de sommet [54], ou d'autres caractéristiques structurelles [62]. Dans ce cas, l'attaque de ré-identification est appelée une « attaque structurelle » qui utilise les informations de structure pour identifier le nœud, où l'adversaire peut utiliser ses connaissances sur la victime, tels que le nombre de ses amis sur un réseau social. En combinant cette connaissance avec la structure de graphe observée, l'adversaire peut inférer une propriété structurelle du sommet. Il peut alors utiliser cette propriété pour partitionner les sommets d'un graphe anonymisé en classes d'équivalence, tel que chaque classe d'équivalence contient les sommets qui ont les mêmes propriétés. Le sommet de la victime est ré-identifié si la classe d'équivalence avec la même propriété de la victime contient un seul sommet [51].

Notons que l'anonymisation naïve prévient la ré-identification quand l'adversaire n'a aucune information sur les individus dans le graphe original [48].

6.1.2 Attaques de réassociation d'informations

Au lieu de publier un graphe social trivialement anonymisé, il est possible de publier un graphe social dans lequel aucune information privée n'est publiée et chaque sommet est associé à une pseudo-identité. Il y a eu un certain nombre d'attaques contre ce type de graphes sociaux en utilisant différents modèles statistiques, des techniques de data mining, et des attaques de sécurité dans le but de découvrir des informations privées cachées d'une victime [51].

• Utilisation de modèles statistiques

Zheleva et Getoor [92] ont présenté un ensemble de modèles d'inférence qui peuvent inférer des valeurs d'attributs sensibles non publiés des utilisateurs dans un graphe social. Le graphe social contient différents types de données sur les utilisateurs, tels que les liens entre les utilisateurs, les appartenances aux groupes, la localisation, et le genre, etc. Les auteurs montrent que la valeur de l'attribut sensible d'un utilisateur non publiée dans le graphe social pourrait être estimée en utilisant les attributs et les relations publiés. Par exemple, en utilisant un modèle d'ami-agrégat, la probabilité de la localisation (non publiée) de la victime peut être estimée à partir des fréquences des localisations des amis de la victime qui ne considèrent pas leurs localisations comme information sensible.

• Utilisation des techniques de data mining

Mao et al. [70] ont noté que les utilisateurs de Twitter ou Facebook révèlent sans le savoir des informations privées dans des tweets ou dans des commentaires. Mao et al ont analysé la divulgation de trois types de tweets privés sur Twitter.com, à savoir, ceux divulguant les plans de vacances, le tweeting sous l'influence de l'alcool, et la révélation des conditions médicales. Ils ont construit des classificateurs pour détecter automatiquement des tweets de ces trois sujets en temps réel et ont démontré que ceci représente une menace réelle pour la vie privée des utilisateurs. Les tweets privés sont publiquement accessibles à partir des sommets dans un graphe social publié, ainsi la détection automatique des informations privées représente une attaque sur les sommets du graphe.

• Utilisation des attaques de sécurité informatique

Les attaques de sécurité informatique traditionnelles peuvent être aussi utilisées pour compromettre la vie privée des individus. Par exemple, l'attaque Sybil [96] peut être utilisée pour pouvoir consulter le profil caché de la victime sur un réseau social. Un site de réseautage social pourrait accorder à un utilisateur le droit de consulter le profil d'un autre utilisateur en fonction de la réputation de l'utilisateur, tel qu'une personne avec une réputation élevée est autorisé à consulter des informations davantage de personnes (ou de manière équivalente une plus grande partie du graphe du réseau social). En utilisant une attaque Sybil un adversaire avec une basse réputation crée un grand nombre d'entités pseudonymes et utilisera ces entités pour augmenter sa propre réputation d'une manière disproportionnée. En conséquence, il peut avoir l'accès aux informations de la victime.

6.2 La divulgation de lien ou la ré-identification de lien

Le problème de la divulgation de lien est centré autour de la protection de la connexion entre les sommets dans un réseau. Deux entités dans un réseau social peuvent avoir une multitude de connexions. Certaines sont sans risque d'être connues au public et d'autres doivent rester privées.

Dans ce type d'attaques l'adversaire est intéressé par la présence ou l'absence d'une arête entre certains nœuds. Il peut identifier l'arête incidente aux sommets de deux personnes cibles en utilisant ses connaissances sur ces personnes pour analyser les caractéristiques topologiques des sommets [55, 32]. Les nœuds du graphe représentent des entités qui sont supposées avoir des relations multiples modélisées par des arêtes. Les arêtes peuvent être de différents types et peuvent être classées comme sensibles ou non sensibles. La ré-identification d'arête ou de lien est une violation à la vie privée parce que les arêtes peuvent représenter des informations sensibles. Parmi les informations sensibles qu'une arête peut porter dans un graphe, nous trouvons deux propriétés d'arête, à savoir le type et le poids d'une relation. Le type définit la nature de la relation, par exemple, une arête peut représenter une amitié, une recommandation, un email ou un appel téléphonique entre deux membres. Le poids définit une mesure quantitative de la relation, par exemple, un poids peut décrire le degré d'une amitié, la fiabilité d'une recommandation, et la fréquence d'une communication, etc. Même sans label, une arête seule peut indiquer l'existence d'une relation. [51]

Notons qu'une arête peut être ré-identifiée même sans pouvoir ré-identifier les sommets [50]. Par exemple, l'adversaire peut connaître les degrés de deux personnes cibles et utiliser cette connaissance pour identifier les classes d'équivalence (CE) de ces deux personnes. Si chaque sommet dans la première CE a une arête avec chaque sommet dans la deuxième CE, l'adversaire peut déduire avec une probabilité de 100% qu'une arête existe entre les deux personnes cibles, même si l'adversaire ne peut pas identifier les deux personnes à l'intérieur de leur CE respective.

6.3 La divulgation de contenu

Généralement, la divulgation de contenu représente un problème lorsque les données privées associées à un utilisateur sur le réseau sont divulguées à des tiers. Un exemple très intéressant concerne le service "Beacon" de Facebook, un système de «publicités sociales" où les préférences de marque et les habitudes de navigation sur Internet, et même les identités sont utilisés pour commercialiser des produits et des services pour un utilisateur donné et ses amis. Par exemple, l'ajout de la dernière saison de « LOST » à votre file d'attente sur « Blockbuster.com » pourrait conduire Facebook à placer une annonce pour Blockbuster directement sur les files d'actualité de vos amis. Ceci peut être intéressant dans certaines situations, mais il peut y avoir certaines choses que l'utilisateur n'est pas prêt à partager avec tout le monde. Du point de vue des utilisateurs, ils veulent demander comment éviter la divulgation de leurs informations privées personnelles tout en profitant de l'avantage de la publicité sociale. Du point de vue de l'entreprise, ils veulent savoir comment assurer aux utilisateurs que leur vie privée n'est pas compromise tout en faisant de la publicité sociale.

La protection contre ce type de divulgation est un problème de recherche et d'ingénierie important. Cependant, le travail dans la littérature à ce jour ne prend pas en compte l'impact des structures de graphes comme les deux autres types de divulgation, mais se concentre

principalement sur quelques techniques traditionnelles de masquage de données pour préserver la vie privée en changeant les données qui doivent être partagées. [60]

7 État de l'art sur les approches d'anonymisation proposées dans la littérature

Nous décrivons dans cette section les modèles existants d'anonymisation des bases de données qui ont été étendus pour l'anonymisation des réseaux sociaux; suivis des différents challenges qui peuvent être rencontrés pour préserver la vie privée des utilisateurs des réseaux sociaux par rapport au cas relationnel. Nous focaliserons par la suite sur les techniques proposées dans la littérature pour préserver la vie privée dans les réseaux sociaux et prévenir les attaques sur les réseaux sociaux naïvement anonymisés.

7.1 Techniques de préservation de privacy dans les bases de données

La préservation de la vie privée est importante dans la publication de données. L'objectif est de publier une version anonymisée des données appartenant à une organisation comme un hôpital, une agence gouvernementale, ou une société d'assurance, sans violation de la vie privée ou divulgation des informations personnelles. Des travaux importants ont été effectués pour préserver la vie privée dans les bases de données relationnelles. Le modèle k-anonymat a été proposé par Samarati et Sweeney [86, 87], pour protéger les informations sensibles lors de la publication des données pour un usage public. Dès lors, une variété de modèles de la vie privée et algorithme d'anonymisation avait été proposés sur la base de k-anonymat, comme la l-diversité [76], le *t-closeness* [9], etc. qui ont montré de bons résultats dans l'anonymisation. La figure 2.4 présente les trois modèles les plus populaires, leurs propriétés et inconvénients.

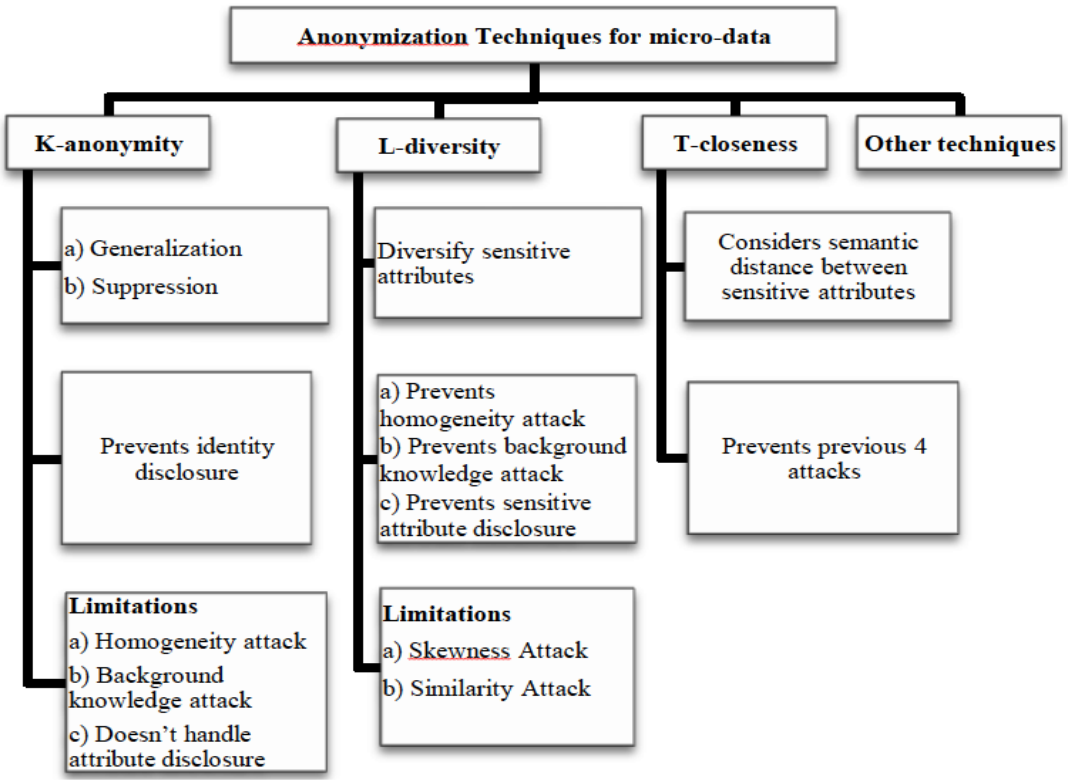


Figure 2.4: Les techniques de préservation de la privacy pour les bases de données [25].

Dans ce chapitre, nous nous concentrons sur les modèles « k-anonymat » et « l-diversité », car ce sont les modèles les plus essentiels et les plus applicables. En particulier, le k-anonymat peut être utilisé même lorsque les attributs sensibles ne sont pas définis. Dans ce qui suit, nous abordons ces deux concepts avec plus de détails.

7.1.1 Le modèle k-anonymat

Le concept de la vie privée sur les données relationnelles a été largement étudié. Une grande catégorie d'attaques contre la vie privée sur les données relationnelles est de ré-identifier les individus en joignant une table publiée contenant des informations sensibles avec certaines tables externes modélisant les connaissances de base des attaquants. Par exemple, la simple élimination des informations d'identification tels que le nom et l'adresse ne suffit pas pour protéger la vie privée, puisque le reste des informations (comme le code postal, genre et date de naissance) peuvent encore ré-identifier une personne de manière unique lorsqu'elles sont combinées avec des informations auxiliaires (tels que les dossiers d'inscription des électeurs).

Pour lutter contre ce type d'attaques (attaques de ré-identification), le concept de k-anonymat a été introduit par Samarati et Sweeney dans [87], et Sweeney dans [86] qui mesure de manière mathématique le degré d'anonymat d'une base de données « anonyme » [86]. Plus précisément, un ensemble de données est dit k-anonyme ($k \geq 1$) si, sur les attributs quasi-identifiant (c'est-à-dire, l'ensemble minimal d'attributs dans la table publiée qui peut être joint avec l'information externe pour ré-identifier les différents tuples), chaque tuple est non distinguable d'au moins (k - 1) autres tuples au sein du même ensemble de données. Plus la valeur de k est grande, meilleure est la protection de la vie privée.

Formellement, le modèle k-anonymat est défini comme suit:
Considérons une table $T = (A_1, \ldots, A_n)$ à publier. Un quasi-identifiant est un ensemble minimal d'attributs $(A_{i1}, \ldots, A_{il})$, $(1 \leq i_1 < \cdots < i_l \leq n)$ dans T qui peuvent être joints avec des informations externes pour ré-identifier les différents tuples de la table. En général, le quasi-identifiant est spécifié par l'administrateur en se basant sur des connaissances de base des adversaires [86].
La table T est dite k-anonyme, étant donné un paramètre k et le quasi-identifiant $(A_{i1},..., A_{il})$ si pour chaque tuple $t \in T$, il existe au moins (k-1) autres tuples $t_1, \ldots, t_{k-1}$ de telle sorte que ces k tuples ont la même projection sur le quasi-identifiant, i.e. $t[A_{i1},...,A_{il}] = t_1[A_{i1},...,A_{il}] = \cdots = t_{k-1}[A_{i1},...,A_{il}]$. Le tuple t et tous les autres tuples indistinguables de t sur le quasi-identifiant forment une classe d'équivalence. [86]

La technique de k-anonymat se base sur la notion de généralisation et de suppression de valeurs. Une généralisation consiste à remplacer une information à caractère personnel avec une autre moins précise mais sémantiquement cohérente. Son principal objectif est de ne pas publier des informations à caractère personnel que s'il y a au moins k individus dans chaque groupe de données généralisées [86]. Par exemple, si on veut appliquer cette technique pour créer un groupe 3-anonymes à partir des informations suivantes :

(30 ans, Annaba, Rhume)
(32 ans, Jijel, Grippe)
(29 ans, Bejaia, Gastroentérite)

On aura la généralisation suivante :
([29-32] ans, Est d'Algérie, Rhume)
([29-32] ans, Est d'Algérie, Grippe)
([29-32] ans, Est d'Algérie, Gastroentérite).

Si *B'* est une base de données *k*-anonyme, un attaquant essayant de joindre *B'* avec une base de données externe *D* non-anonyme, il trouve au moins *k* enregistrements correspondants dans *B'* quelle que soit la valeur utilisée du quasi-identifiant.

7.1.2 Le modèle l-diversité

Bien que le k-anonymat ait été bien adopté, Machanavajjhala et al [76] ont montré qu'un ensemble de données k-anonyme a quelques problèmes de privacy importants dû au manque de diversité dans les attributs sensibles. En particulier ils ont montré que le degré de protection de la vie privée ne dépend pas vraiment de la taille des classes d'équivalence sur les attributs quasi-identifiant qui contiennent des tuples identiques sur ces attributs. Au lieu de cela, il est déterminé par le nombre et la répartition des valeurs sensibles distinctes associées à chaque classe d'équivalence. Pour surmonter la faiblesse de k-anonymat, ils ont proposé la notion de l-diversité [76]. Xiao et Tao [83] ont prouvé que la technique d'anonymisation l-diversité garantit toujours plus fortement la préservation de la vie privée que le k-anonymat dans la mesure où elle garantit en plus que dans un groupe de k individus qu'il y'aura au moins *l* valeurs sensibles distinctes. En effet, si cette vérification n'est pas effectuée, il se pourrait que la valeur sensible associée à un individu puisse être retrouvée, bien que cet individu ait été anonymisé par la technique de k-anonymat.

Comme exemple, les données suivantes sont « 3-anonymes et 1-diverses » :
{([29-32] ans, Est d'Algérie, Rhume) ;
([29-32] ans, Est d'Algérie, Rhume) ;
([29-32] ans, Est d'Algérie, Rhume)}

On remarque que, si on sait qu'une personne a un âge entre « 29 et 32 » ans et habite en région «Est d'Algérie» alors on peut déduire à 100% qu'elle a un « rhume ».

Par contre, dans les données suivantes « 3-anonymes et 3-diverses » on peut rien inférer :
([29-32] ans, Est d'Algérie, Rhume)
([29-32] ans, Est d'Algérie, Grippe)
([29-32] ans, Est d'Algérie, Gastroentérite).

En conclusion, de nombreux modèles de préservation de la vie privée et d'anonymisation ont été proposés pour les données relationnelles. La généralisation et la perturbation sont deux techniques de base populaires utilisés pour anonymiser les données relationnelles. Dans le contexte de réseau social, des travaux ont été effectués par divers chercheurs utilisant le k-anonymat, la l-diversité et les approches intégrant les deux modèles pour protéger les données des utilisateurs du réseau social tout en les publiant en ligne. Comme déjà présenté, les données du réseau social sont représentées sous forme de graphe où chaque nœud/sommet représente un individu et les arêtes représentent les liens entre les nœuds. Les techniques de préservation de la vie privée sont basées sur cette notion de graphe [25]. Cependant l'anonymisation des données de réseau social est beaucoup plus difficile. La section suivante montre les différents challenges dans l'anonymisation des réseaux sociaux comparant au cas relationnel largement étudié.

7.2 Challenges (Anonymisation des réseaux sociaux VS anonymisation des bases de données)

Les méthodes d'anonymisation des données relationnelles ne peuvent pas être appliquées directement aux données de réseaux sociaux étant donné que le réseau social est une structure complexe de sommets et d'arêtes. Il y a donc un besoin de développer une méthode systématique pour anonymiser les données de réseau social avant qu'il ne soit publié. Toutefois, l'anonymisation des données de réseau social est beaucoup plus difficile que l'anonymisation des données relationnelles pour les raisons suivantes : [54]

Premièrement, il est beaucoup plus difficile de modéliser les connaissances de base des adversaires ainsi que les attaques sur les réseaux sociaux que celles sur les bases de données relationnelles. Dans le cas relationnel, il est souvent supposé qu'un ensemble d'attributs non sensibles appelés les quasi-identifiants est utilisé pour associer des données provenant de plusieurs tables, et les attaques proviennent principalement de la ré-identification des individus et leurs attributs sensibles à partir de cet ensemble d'attributs quasi-identifiant. Cependant, dans un réseau social de nombreuses informations peuvent être utilisées pour identifier les individus, tels que les labels des sommets et d'arêtes, le degré ou le graphe de voisinage d'un nœud, les sous-graphes induits, ainsi que leurs combinaisons.

Deuxièmement, la mesure de la perte de l'information dans l'anonymisation des données de réseaux sociaux est beaucoup plus difficile que celle dans l'anonymisation des données relationnelles. En général, la perte d'information dans une table anonymisée peut être mesurée tuple par tuple. Étant donné un tuple dans la table d'origine et le tuple correspondant dans la table anonymisée, nous pouvons calculer la distance entre les deux tuples pour mesurer l'information perdue au niveau du tuple, la somme de la perte d'information dans les différents tuples est utilisée pour mesurer la perte d'information au niveau de la table. Cependant, un réseau social est constitué d'un ensemble de sommets et un ensemble d'arêtes, nous ne pouvons pas comparer deux réseaux sociaux en comparant les sommets et les arêtes individuellement. Deux réseaux sociaux peuvent êtres très différents même s'ils ont le même nombre de sommets et le même nombre d'arêtes. Par conséquent, nous devons considérer plusieurs propriétés du réseau telles que la connectivité, l'intermédiarité, le diamètre, et la structure du réseau. Ainsi, il peut y avoir plusieurs manières de définir les mesures de la perte d'information ainsi que la qualité de l'anonymisation.

Troisièmement, concevoir des méthodes d'anonymisation pour les données de réseau social doit être différente que celles pour les données relationnelles. Les méthodes « Divide-and-conquer » ou «diviser et conquérir » sont largement appliquées dans l'anonymisation des données relationnelles du fait que les tuples dans une table relationnelle sont séparables durant la phase d'anonymisation. En d'autres termes, l'anonymisation d'un groupe de tuples n'affecte pas les autres tuples de la table. Cependant, les méthodes « Divide-and-conquer » ne peuvent pas être utilisées pour les données du réseau social car le changement des labels de sommets et d'arêtes peut affecter les voisinages d'autres sommets, et la suppression ou l'ajout de sommets et d'arêtes peut affecter d'autres sommets et arêtes, ainsi que les propriétés du réseau. Par conséquent, des techniques spécifiques doivent être proposées pour anonymiser les données de réseaux sociaux.

7.3 Techniques de préservation de privacy dans les réseaux sociaux

Afin de lutter contre les attaques actives et passives et prévenir les attaques de connaissances externes sur les réseaux sociaux naïvement anonymisés, il existe plusieurs approches d'anonymisation proposées dans la littérature, qui ont été présentées comme une nécessité en plus de l'anonymisation naïve pour préserver la vie privée tout en publiant les données du réseau social. Ces approches ont été classées par Bin Zhou et al dans [32] en deux catégories : « Approches par modification de graphe » et « Approches basées sur le clustering ». Dans la première catégorie des arêtes et/ou des sommets sont généralement ajoutés et/ou supprimés pour que le graphe satisfasse certaine conditions d'anonymat. La plupart de ces approches implémentent le modèle k-anonymat [86] sur différentes connaissances de base de l'attaquant. La deuxième catégorie basée sur le Clustering consiste à regrouper les sommets et les arêtes pour former des « super nœuds » et des «super arêtes» et anonymiser les sous-graphes dans les « super nœuds » [32]. Chaque « super arête » représente plus d'une arête dans le graphe original et chaque super-nœud représente un certain groupe de nœuds qui s'appelle également un «cluster». La topologie d'un groupe n'est pas révélée, mais seulement le nombre de nœuds groupés et le nombre d'arêtes entre eux, ainsi que le nombre d'arêtes qui le raccordent avec d'autres super-nœuds.

Toutes les approches proposées présentent la structure suivante : [73]
Premièrement, elles considèrent un certain modèle de l'adversaire (les informations privées cibles d'attaques et les connaissances de l'adversaire) qui influe sur l'efficacité de la solution proposée, c'est-à-dire, considérer des adversaires puissants (ou faibles) conduit à des techniques d'anonymisation robustes (ou fragiles). Ensuite, une technique d'anonymisation est proposée, basée sur une notion de privacy, telle que le k-anonymat. Dernièrement, la technique est évaluée pour estimer l'utilité de l'ensemble des données anonymisées et/ou le niveau de privacy fourni par la technique proposée.

Il y a eu des travaux importants sur la façon d'appliquer le modèle k-anonymat pour protéger les identités des sommets dans les réseaux sociaux publiés contre diverses attaques [48, 60, 54, 63] dans lesquelles la connaissance préalable maîtrisée par un attaquant peut être le degré d'un nœud ou encore tout sous-graphe arbitraire donné qui couvre un utilisateur cible. Le but est de publier un graphe social, qui a toujours au moins k candidats dans différents scénarios d'attaques. En fonction de la connaissance qu'un adversaire utilise pour attaquer le nœud cible les chercheurs ont développé de nombreux modèles de protection de la vie privée basés sur le k-anonymat. Cependant, même quand ces modèles de privacy sont respectés, un attaquant peut être capable encore de déduire des informations privées si un groupe de nœuds partage largement les mêmes labels sensibles. En d'autres termes, la relation label-nœud n'est pas bien protégée par les méthodes d'anonymisation de structure pure [79]. Par conséquent, le k-anonymat n'est pas suffisant pour protéger contre la divulgation d'attributs sensibles. Ainsi, le modèle l-diversité [76] a été suggéré d'être appliqué pour contrer ce problème. Nous présentons ci-dessous quelques exemples d'approches d'anonymisation de réseau social basées sur ces deux concepts « k-anonymat » et « l-diversité ».

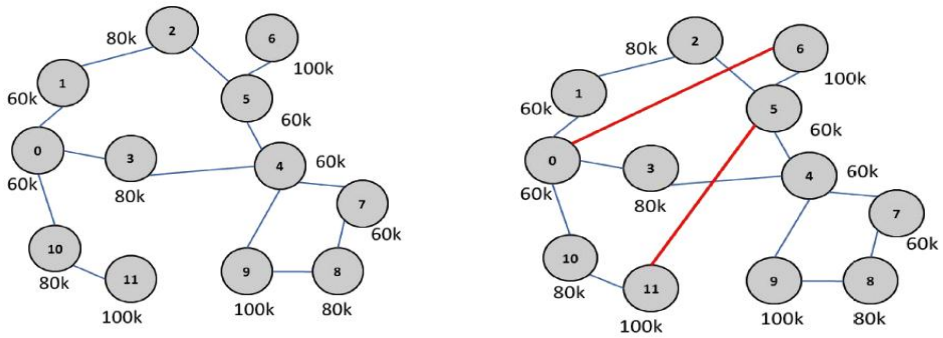
7.3.1 Le modèle « k-candidat »

Hay et al [62, 48] ont examiné le problème de la ré-identification d'un individu connu dans le réseau naïvement anonymisés. Ils ont observé que la similarité structurelle des nœuds dans le graphe et les connaissances de base qu'un attaquant peut obtenir conjointement détermine à quel point un individu peut être distingué. Ils ont modélisé les connaissances de base des

adversaires comme des requêtes structurelles, et ils ont proposé un nouveau concept d'anonymisation des graphes sociaux basé sur la notion de k-anonymat [87] « l'anonymat de k-candidat ». Comme proposé dans [62], un graphe social anonymisé satisfait le k-anonymat si, pour une propriété donnée d'un nœud donné, (par exemple, le degré du nœud, les degrés des voisins d'un nœud, etc.) il y a dans le graphe au moins (k-1) autres nœuds avec une telle propriété. Comme résultat de cela, la meilleure chose qu'un adversaire peut faire avec des connaissances externes sur le graphe social est d'identifier un ensemble de k nœuds candidats dans l'ensemble de données publiées qui pourraient correspondre à un individu identifiable. Ils ont développé une méthode de perturbation aléatoire de graphe en supprimant ou en ajoutant aléatoirement des arêtes. Leur modèle suppose que les nœuds et les arêtes dans un réseau social ne sont pas étiquetés.

7.3.2 Le modèle « k-degee » et « KDLD »

Liu et Terzi [53] ont considéré le scénario de divulgation d'identité où les identités des individus associés aux sommets sont révélées. Ils ont introduit le concept d'anonymat du « k-degré » pour prévenir les attaques de ré-identification possibles des individus en utilisant la connaissance préalable du degré d'un sommet de la victime. Par exemple, dans la figure 2.5(a), si un adversaire sait qu'une personne a quatre amis, il peut immédiatement savoir que le nœud 4 représente cette personne et ainsi les attributs relatifs au nœud 4 sont révélés même si les identités des nœuds sont supprimées à la publication des données du réseau.



(a) : Le graphe original **(b)** : graphe anonyme 3-degré

Figure 2.5 : Modèle d'anonymisation « k-degré »

Si nous voyons la figure 2.5(b), l'adversaire ne peut pas conclure que le nœud 4 représente cette personne, le graphe est 3-degré anonyme. Un graphe est dit k-degré anonyme si et seulement si pour chaque nœud v, il existe au moins (k-1) autres nœuds dans le graphe avec le même degré que v. Leur méthode d'anonymisation consiste à modifier le graphe en ajoutant et en supprimant des arêtes du graphe pour atteindre l'anonymat de k-degré.

Yuan et al. [79] ont défini le modèle d'anonymat KDLD « k-degree l-diversity » qui considère la protection de l'information structurelle « degré » ainsi que les labels sensibles des individus.

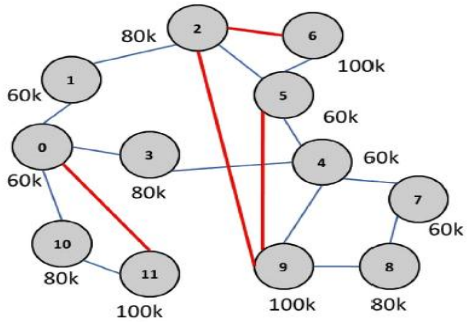


Figure 2.6 : graphe 3-degré-3-diverse

Considérons le même exemple du graphe de la figure 2.5, quand le graphe du réseau social contient des nœuds avec des attributs sensibles (exemple : les salaires), appliquer seulement le modèle d'anonymat « *k-degree* » n'est pas suffisant pour prévenir l'attaque d'inférence des attributs sensibles. La figure 2.5(b) montre un graphe qui satisfait le modèle d'anonymat « *3-degré* » mais les labels de nœuds ne sont pas considérés. Dans ce cas, les nœuds 0, 4, 5 ont le même degré 4, mais ils ont tous le même label « 60k ». Si un attaquant sait que quelqu'un a 4 amis dans le réseau social, il peut conclure que le salaire de cette personne est « 60k » sans exactement ré-identifier son nœud. Pour résoudre ce problème, Yuan et al.[79] ont proposé le modèle d'anonymat KDLD, un graphe est KDLD anonyme si et seulement si pour chaque nœud dans ce graphe il existe au moins (k-1) autres nœuds ayant le même degré et au moins l valeurs de labels sensibles distinctes dans chaque classe d'équivalence (la figure 2.6 montre un graphe anonyme *3-degré-3-diverse*). La méthode d'anonymisation proposée est basée sur l'ajout de faux nœuds dans le graphe original en prenant en considération d'introduire le moins possible de distorsion aux propriétés du graphe.

Jia et al dans [81] ont développé un modèle d'anonymat PKDLD « personalized k-degree-l-diversity » pour personnaliser la persévération de la vie privée dans la publication de données de réseau social. En divisant les nœuds selon des exigences différentes de vie privée, ils ont pu réduire le coût de la distorsion de graphe et améliorer l'utilité des données.

7.3.3 Approches d'anonymisation des voisinages

Zhou et Pei [54] ont identifié un type essentiel d'attaques: « les attaques de voisinage ». Ces attaques sont possibles quand un adversaire a des connaissances sur les voisins d'une victime cible et les relations entre ces voisins. Ils ont proposé le modèle d'anonymat « k-neighborhood » ou « k-voisinage ». Pour un graphe social G, supposons qu'un adversaire connaît la structure de voisinage d'un sommet u ∈ V (G), dénoté par $Neighbor_G(u)$. Si $Neighbor_G(u)$ a au moins k copies isomorphes dans G' où G' est le graphe anonymisé de G, alors u ne peut être ré-identifié dans G' avec une probabilité supérieure à 1/k. La technique d'anonymisation proposée est basée sur l'ajout des liens pour atteindre le k-voisinage. Les auteurs ont proposé les codes DFS et les codes DFS minimaux comme technique de codage pour les sous-graphes de voisinage. Ils ont limité leur étude au cas où seulement les voisins immédiats (voisins à un saut) sont considérés, c.-à-d. seulement les sommets dans $Neighbor_G(u)$. Ils ont effectué une étude empirique qui indique que les réseaux sociaux anonymisés générés par leur méthode peuvent être utilisés pour répondre aux requêtes d'agrégation. Dans notre travail nous nous intéressons à ce type d'attaque.

Toujours pour prévenir « les attaques de voisinage », Tripathy et al [64] ont modifié convenablement l'algorithme proposé par Zhou et Pei [54] pour gérer également le cas des

voisins à plusieurs sauts, en utilisant les matrices d'adjacence comme technique de représentation des voisinages (au lieu les codes DFS) dont ils ont prouvé son efficacité ainsi sa complexité minimale par rapport au codes DFS. L'utilité considérée a été toujours pour répondre aux requêtes d'agrégation.

Lan et al. [77] ont développé un algorithme appelé KNAP « *K-Neighborhood Anonymous Publication* » contre l'attaque de voisinage. La différence avec les autres méthodes d'anonymisation c'est que les technologies existantes se concentrent sur une approche universelle qui exerce le même niveau de la préservation pour toutes les entités, sans couvrir leurs besoins concrets. Lan et al [77] présentent une méthode *k*-n*eighborhood* basée sur le concept d'anonymat personnalisée en divisant les entités en entités sensibles et non sensibles. Les entités déclarent leurs exigences de vie privée lors de la soumission des données.

Dans le papier [78], Zhou et al vont au-delà du « k-anonymat » et implémentent le concept de « l-diversité ». Dans ce cas, chaque sommet est associé à certains attributs non sensibles et certains attributs sensibles. Si un adversaire peut ré-identifier les valeurs d'attributs sensibles d'une cible donné avec une probabilité élevée, la vie privée de cette personne est violée. Zhou et al ont proposé une technique basée sur l'ajout/la suppression d'arêtes dans le but de réaliser un graphe k-anonyme et l-diverse (modèle *k-neighborhood-l-diversity)* pour protéger les labels sensibles. Un graphe *l*-diverse s'assure que l'adversaire ne peut pas inférer les valeurs d'attributs sensibles avec une probabilité supérieure à 1/*l*.

7.3.4 Le modèle « k-automorphisme »

Zou et al. [63] ont adopté une hypothèse plus générale : Ils supposent que l'adversaire peut avoir la connaissance de tout sous-graphe autour d'un certain individu. Si un tel sous-graphe pourrait être identifié dans le graphe publié avec une forte probabilité, l'utilisateur a un risque élevé de divulgation d'identité. Les auteurs dans leur travail ont présenté un examen complet des techniques d'anonymisation précédentes, critiquant que la plupart d'entre elles ont été conçues soit pour résister à un seul type d'attaques, soit pour offrir un graphe anonymisé qui souffre d'une importante perte d'utilité. Ils ont proposé un modèle de protection « k-automorphisme » : un graphe est dit k-automorphisme si et seulement si, pour chaque sommet dans le graphe publié il existe au moins (k-1) autres sommets ayant les mêmes propriétés structurelles (aucune différence de structure), peu importe la quantité d'information structurelle que l'adversaire dispose, c.à.d. pour tout sous-graphe $S \in G$, G' son graphe anonymisé contient au moins (k-1) sous-graphes isomorphes à S. Les réseaux considérés dans [63] sont des réseaux non étiquetés (sans labels).

7.3.5 Approches d'anonymisation de liens

D'autres travaux se concentrent sur le problème de divulgation de lien [61, 55, 50, 75,108] qui détermine s'il existe un lien entre deux individus ou non. Semblable aux méthodes d'anonymisation de sommet, les méthodes d'anonymisation d'arête protègent les informations privées sensibles associées à cette arête. L'anonymisation d'arêtes est plus difficile par rapport à l'anonymisation de sommets parce que la confidentialité d'une arête peut encore être violée même si le graphe satisfait une condition d'anonymat de sommets. Le problème est que les méthodes d'anonymisation de sommets considèrent chaque sommet indépendamment et la dissimulation de deux sommets ne garantit pas la dissimulation de l'existence d'une arête entre ces deux sommets.

Considérons la figure 2.7 comme exemple, la Figure 2.7(a) est un petit graphe social dans lequel les sommets représentent des personnes et les arêtes représentent des communications par courriers électroniques, les numéros à l'intérieur des cercles représentent les identifiants des sommets qui sont affectés aléatoirement. Supposons que Ed et Gary veulent cacher leurs communications et désignent l'arête entre eux (la ligne épaisse) comme sensible. La figure 2.7(b) est un graphe 2-anonyme en terme de degré de sommets obtenu à partir de celui présenté dans la figure 2.7(a). Les numéros à l'extérieur des cercles représentent les degrés des sommets. Supposons qu'un adversaire veut savoir s'il y a un email envoyé entre Ed et Gary. Supposons que l'adversaire sait que Ed a des courriels avec trois personnes (donc son sommet devrait avoir un degré de trois) et que Gary a des courriels avec quatre personnes (c'est à dire, son sommet devrait avoir un degré de quatre). En partitionnant le graphe de la figure 2.7(b) en utilisant les degrés des sommets, l'adversaire pouvant obtenir trois classes d'équivalence de sommets, i.e. $CE_1 = \{v_1; v_2; v_3; v_4; v_6\}$, $CE_2 = \{v_5; v_8\}$ et $CE_3 = \{v_7; v_9\}$. En observant la figure 2.7(b), l'adversaire peut seulement dire qu'Ed est dans CE_2 et Gary est dans CE_3, mais ne peut pas dire lequel entre v_5 et v_8 représente Ed et lequel entre v_7 et v_9 représente Gary. Ainsi la ré-identification de sommet est empêchée. Cependant, l'adversaire peut déduire avec certitude de 100% qu'il y a une communication par courrier électronique entre Ed et Gary parce que chaque sommet dans CE_2 a une arête avec chaque sommet dans CE_3.

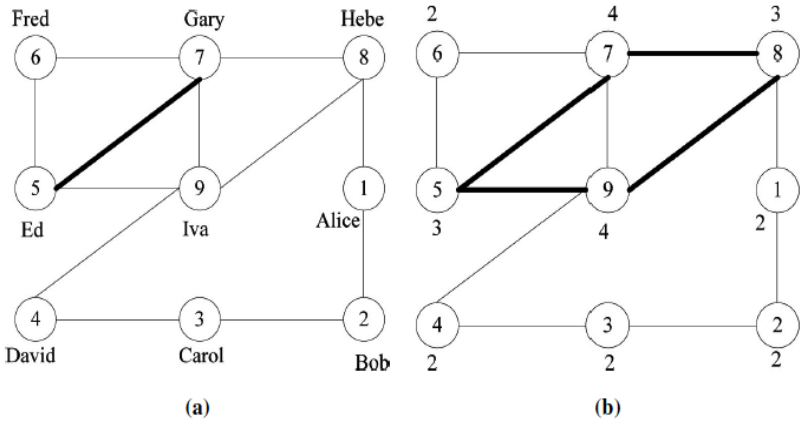


Figure 2.7 : Exemple de révélation de relation sensible

Zheleva et Getoor dans [61] ont abordé le problème de ré-identification de lien qu'ils le définissent comme étant l'inférence des relations sensibles à partir des relations non sensibles. Ils se sont concentrés sur les réseaux sociaux où les nœuds ne sont pas étiquetés, mais les arêtes sont étiquetées. Ils ont considéré deux types d'arêtes; arêtes sensibles qui doivent être cachées et arêtes non sensibles. Pour protéger les arêtes sensibles cinq stratégies différentes de clustering basées sur des opérations d'ajout/suppression d'arêtes ont été proposées. L'objectif est d'atteindre la protection des informations d'arêtes, tout en produisant des données anonymisées utiles. L'utilité est mesurée par le nombre d'arêtes non sensibles supprimées.

Zhang et al. [50] supposent que l'adversaire connaît certaines descriptions de sommets comme les degrés et proposent de réduire la probabilité de l'existence d'une arête reliant deux individus par la permutation et la suppression d'arêtes. L'approche ne considère pas la résistance à la ré-identification de sommets. Par conséquent, il est possible qu'une victime peut être uniquement ré-identifiée, même si la probabilité qu'une arête relie la victime et son ami est faible.

Cheng et al. [69] ont conçu le modèle « k-isomorphisme » pour protéger les liens ainsi que les sommets contre un adversaire ayant la connaissance de sous-graphe. Semblable à [63], ils n'imposent pas de restrictions sur la taille d'un sous-graphe.

Avec une approche différente, Ying et Wu [55] ont étudié la ré-identification de lien sans considérer les connaissances de base d'adversaire. Pour l'anonymisation, ils ont proposé l'ajout, la suppression et la permutation aléatoire d'arêtes. Leur technique vise à minimiser la perturbation des propriétés spectrales du graphe original.

Li et al. [75] ont proposé de protéger une relation privée entre deux utilisateurs dans l'un peut être identifié dans les données de réseau social publié. Le modèle d'anonymisation de l-diversité a été défini pour préserver la confidentialité des relations des utilisateurs. Deux algorithmes de manipulation de graphe MaxSub et MinSuper, ont été proposés pour atteindre la l-diversité.

7.3.6 Approches d'anonymisation de graphes dynamiques

Dans [90] une faiblesse des études antérieures sur l'anonymisation est mentionnée : dans le domaine de l'anonymisation des réseaux sociaux, la concentration a été seulement sur la protection des informations personnelles d'une seule instance du réseau publié dans un moment précis, et ceci est incompatible avec la nature très dynamique de ces réseaux. Les réseaux sociaux en ligne évoluent et une seule instance est insuffisante pour analyser leur évolution ou leurs données. Cependant, publier plusieurs copies de données anonymisées d'un réseau social, qui sont prises à des instants différents pour donner des informations sur comment le réseau évolue peut conduire à la révélation d'informations sensibles si l'adversaire compare ces copies. [90]

A cet effet, il existe des méthodes pour anonymiser un réseau dynamique lorsque de nouveaux nœuds et arêtes sont ajoutés au réseau publié. Ces méthodes utilisent l'algorithme de prédiction de liens pour modéliser l'évolution du réseau (c'est-à-dire, une prévision de changements topologiques sur le réseau social ou définition informelle : prédire la formation d'un lien entre deux nœuds jamais connectés auparavant). Par l'utilisation de ce graphe prévu pour effectuer l'anonymisation, la perte de la vie privée causée par les nouvelles arêtes peut être éliminée presque entièrement. [59]

8 Conclusion

Beaucoup d'études ont été faites pour la préservation des informations privées lors de la publication des données du réseau social. Dans la littérature [62], Hay et al ont proposé l'anonymisation naïve, qui remplace les attributs d'identification des individus dans un réseau avec des identifiants synthétiques aléatoires avant de publier les données. Bien que le réseau naïvement anonymisé permet une analyse utile et les propriétés globales du réseau sont conservées, comme souligné dans [62, 47], Backstrom et al [47] ont montré que cette approche simple peut être insuffisante puisqu'un adversaire pourrait encore ré-identifier le nœud d'une personne cible sur le graphe anonymisé. En exploitant des connaissances préalablement collectées sur l'individu cible, l'adversaire peut même apprendre l'existence

d'une relation sociale entre deux nœuds ré-identifiés ou encore utiliser la structure du graphe elle-même pour déduire la valeur de certains attributs sensibles.

L’anonymisation est un processus crucial pour assurer que les données publiées du réseau social ne révèlent pas des informations sensibles sur les utilisateurs. Plusieurs approches d’anonymisation ont été proposées dans la littérature, ces approches ont été présentées comme une nécessité en plus de l’anonymisation naïve pour préserver la vie privée tout en publiant les données du réseau social et prévenir les différentes attaques possibles sur ces réseaux.

Dans le prochain chapitre, nous allons présenter notre nouvelle approche d’anonymisation proposée pour contrer les attaques de voisinage qui a pour but par rapport aux approches existantes, de préserver les propriétés structurelles des graphes anonymisés.

1 Introduction

Actuellement, de plus en plus les données du réseau social sont mises à disposition du public d'une manière ou d'une autre, protéger les informations personnelles tout en publiant les données du réseau social devient une préoccupation très importante. Avec quelques connaissances locales sur les individus dans un réseau social, un adversaire peut violer facilement la vie privée de certaines victimes. Est-il possible que la publication des données de réseaux sociaux, même avec des individus anonymes, menace encore la vie privée ?
Beaucoup de réseaux sociaux recueillent des informations confidentielles sur leurs utilisateurs, des informations qui pourraient potentiellement être employées improprement. Par exemple, dans le domaine de la santé, PatientsLikeMe[20], un réseau social avec plus de 150.000 utilisateurs à partir de Juillet 2012, crée des communautés de patients pour diverses maladies. Tels que les patients peuvent échanger des informations sur leur maladie, leur traitement et leur expérience. En raison de cette quantité de données sensibles recueillies par les sites de réseaux sociaux, la divulgation de la vie privée est devenue un sujet de préoccupation pour de nombreux utilisateurs, et la recherche dans ce domaine a prospéré au cours des dernières années.

Le développement des réseaux sociaux en ligne et la publication des données de réseau social a entraîné un risque de fuite d'informations personnelles des individus (exemple : salaire, maladie, connexion à un groupe spécifique, etc.) (Voir figure 3.1). Cela nécessite la préservation de la vie privée avant que de telles données soient publiées. Dans notre travail, nous nous intéressons à un type important d'attaques contre la vie privée dans les réseaux sociaux: « les attaques de voisinage ». Si un adversaire possède une certaine connaissance sur les voisins d'une victime cible et les relations entre ces voisins, la victime peut être ré-identifiée même si l'identité de la victime est préservée à l'aide des techniques conventionnelles d'anonymisation.

La plupart des études antérieures sur la préservation de la vie privée peuvent traiter seulement les données relationnelles, et ne peuvent pas être appliqué directement aux données des réseaux sociaux. Cependant, Bin Zhou et Jian Pei [54] ont proposé une méthode d'anonymisation d'un réseau social pour prévenir la ré-identification des nœuds à travers l'information structurelle « voisinage », qui est une initiative dans cette direction et qui fournit une solution pratique au problème. Par la suite, d'autres travaux de recherche ont été aussi proposés pour résoudre le même problème comme dans [64, 78,77]. En fait, les solutions existantes répondent aux besoins d'anonymat mais dans certains cas peuvent modifier de manière significative les propriétés du graphe original notamment la distance entre les différents nœuds.

L'étude approfondie de l'attaque de voisinage nous a permis de bien comprendre l'approche d'anonymisation proposée par Zhou et Pei contre ces attaques. Cette approche, qui fonctionne à base du principe de l'ajout des liens pour avoir des voisinages isomorphes préserve considérablement la vie privée contre les attaques de voisinage mais peut modifier significativement les propriétés structurelles du graphe original et donc son utilité potentielle. Notre problématique s'inscrit dans ce contexte, à savoir la protection de la vie privée tout en préservant une propriété structurelle très importante à savoir « APL ». La préservation d'une telle propriété dans l'anonymisation pourrait être extrêmement essentielle par la suite pour l'analyse des graphes des réseaux anonymisés.

[20] http://www.patientslikeme.com, depuis 2005.

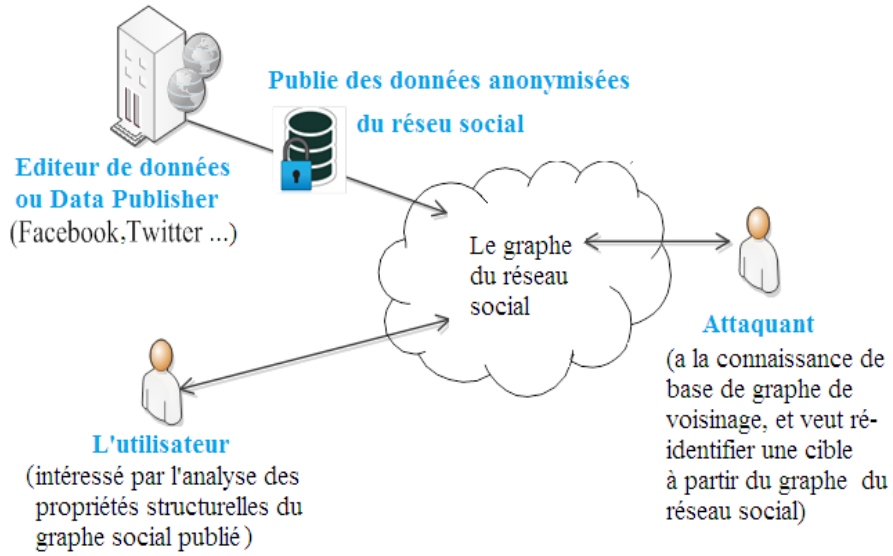
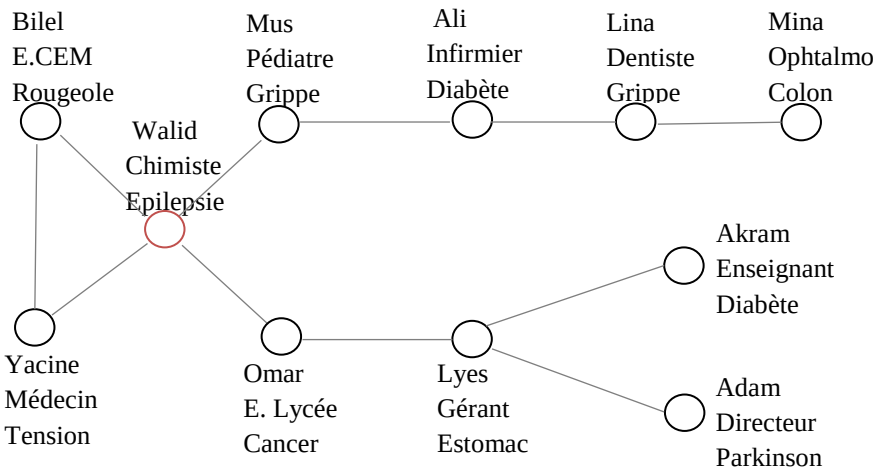


Figure 3.1 : Publication des données de réseau social

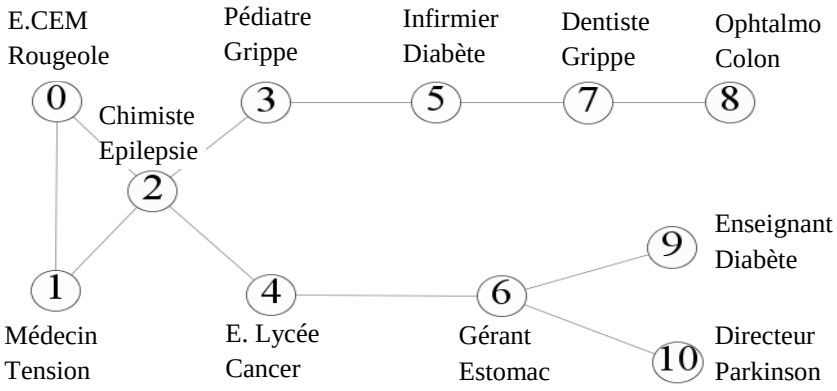
Dans ce chapitre, nous allons proposer une nouvelle approche d'anonymisation de réseau social qui préserve autant que possible la propriété de la distance moyenne ou APL. Nous commençons par une illustration de l'attaque de voisinage pour montrer comment un attaquant peut identifier une personne dans le graphe publié en utilisant sa connaissance de voisinage. Par la suite, nous discutons les limites de la solution existante pour prévenir cette attaque, et nous présentons notre contribution pour améliorer cette solution.

2 Illustration des attaques de voisinage

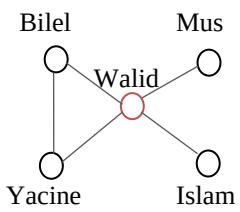
Comme exemple concret, prenons un réseau social synthétisé des « amis» représenté sur la figure 3.2(a). Chaque sommet dans le réseau représente une personne. L'attribut sensible associé à chaque nœud du réseau représente une maladie, et l'attribut non sensible représente la profession de chaque personne. Une arête relie deux personnes qui sont des amis. Supposons que le réseau doit être publié. Pour préserver la vie privée, est-il suffisant de supprimer toutes les identités comme le montre la figure 3.2(b) (autrement dit effectuer une anonymisation naïve, où les identifiants sont remplacés par des nombres aléatoires) ?
Malheureusement, si un adversaire a quelques connaissances sur les voisins d'un individu, la vie privée peut être divulguée. Si un adversaire veut trouver des informations sur « Walid » et sait qu'il a deux amis qui se connaissent et deux autres amis qui ne se connaissent pas, c.-à-d. il connait le graphe de voisinage de « Walid » comme illustré dans la figure 3.2(c) alors le sommet « 2 » représentant « Walid » peut être identifié de manière unique dans le réseau puisqu'aucun autre sommet n'a le même graphe de voisinage. L'adversaire peut ainsi savoir que « Walid » souffre d'épilepsie. Ceci représente une intrusion de la vie privée de « Walid ». De même, « Lyes » peut être identifié dans la figure 3.2(b) si l'adversaire connaît le graphe de voisinage de « Lyes».



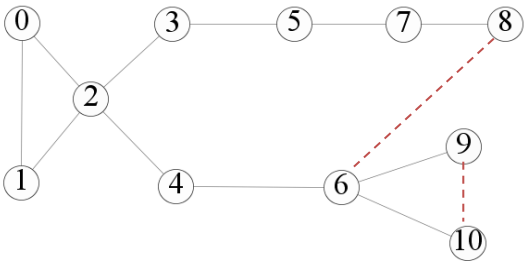
(a) : Le réseau social



(b) : Le réseau avec des nœuds anonymes



(c) : Le graphe de voisinage de Walid



(d) : Un réseau 2-anonyme en ajoutant des liens

Figure 3.2 : Les attaques de voisinage dans un réseau social

Identifier des individus dans les réseaux sociaux publiés viole la vie privée. Dans cet exemple, par l'identification de « Walid » et « Lyes », un adversaire peut même connaître à partir du réseau publié (la figure 3.2(b)) que « Walid » et « Lyes » partagent un ami en commun. D'autres informations privées peuvent être ensuite inférées telles que la façon dont une victime est connectée au reste du réseau et la position relative de la victime par rapport au centre du réseau, etc.

Maintenant, supposons que l'adversaire veut trouver des informations sur « Lina » et sait qu'elle a deux amis qui ne se connaissent pas dans le réseau. Utilisant cette connaissance, il essaie de la trouver dans le réseau. Il y a 4 sommets dans le réseau qui ont le même voisinage : 5, 7, 3 et 4 comme représenté sur la Figure 3.2(b). « Lina » peut être n'importe qui parmi ces derniers. Ainsi, « Lina » ne peut pas être identifiée dans le réseau social avec une probabilité supérieure à 1/4. Si chaque nœud dans le réseau social ne peut être identifié avec une probabilité supérieure à 1 / k, le réseau est dit qu'il suit le principe de « k-anonymat » [86]. L'attaque utilisée ici est appelée attaque de ré-identification en utilisant l'information structurelle « voisinage ». Dans ce type d'attaques, l'adversaire correspond ses connaissances de base à un réseau naïvement anonymisé.

3 Contribution

Pour protéger la vie privée de manière satisfaisante, une solution est de garantir que tout individu ne puisse pas être identifié correctement dans le réseau social anonymisé avec une probabilité supérieure à 1/k, où k est un paramètre spécifié par l'utilisateur portant les mêmes caractéristiques du modèle k-anonymat de L.Sweeney [86]. Dans l'exemple de la figure 3.2, un graphe « 2-neighborhood » ou « 2-voisinage » anonyme de la figure 3.2(a) généré par l'ajout de liens peut être publié. En ajoutant deux faux liens, un reliant « Lyes » et « Mina » et l'autre reliant « Akram» et « Adam », le graphe de voisinage de chaque sommet dans la figure 3.2(d) n'est plus unique. Un adversaire avec la connaissance de voisinage d'un nœud, obtient toujours au moins deux nœuds candidats, donc il ne peut pas identifier un individu dans ce graphe anonyme avec une probabilité supérieure à ½.
Zhou et Pei [54] ont pris l'initiative d'aborder le problème de préservation de la vie privée dans la publication des réseaux sociaux contre les attaques de voisinage, et ont proposé une méthode d'anonymisation basée sur l'ajout des liens, et par la suite, d'autres travaux de recherche [64,77,78] ont été apparus qui ont basé sur la solution de Zhou et Pei [54], mais les méthodes d'anonymisation existantes peuvent causer des erreurs significatives dans certaines tâches d'analyse des propriétés structurelles telles que la distance entre certaines paires de nœuds , la mesure de distance moyenne « APL », le diamètre, le rayon, etc.

Par exemple en reliant « Lyes » et « Mina » la distance entre les nœuds 6 et 8 est modifiée de 6 à 1 dans la figure 3.2(d). Nous notons que cet ajout de lien a modifié significativement la valeur de la distance et par conséquent, toute analyse (data mining) sur ces données pourrait obtenir des conclusions erronées ou non valides.

L'avantage de la méthode d'ajout de liens déjà proposée maintient les nœuds dans le graphe original inchangés, cependant, elle peut largement affecter la structure du graphe. Cette méthode peut parfois modifier les propriétés de distance sensiblement par exemple en reliant deux nœuds lointains qui appartiennent à deux communautés différentes.

Pour mieux expliquer cet exemple, considérons que la structure des communautés peut être détectée à partir des relations d'amis dans le réseau social. Supposons que 6 et 8 sont des membres de deux communautés différentes dans le graphe original, et les communautés sont loin les uns des autres. En connectant 6 à 8, ces communautés peuvent devenir très proches ou être fusionnées pour former une seule communauté.

Ainsi, compter uniquement sur l'ajout de liens ne peut pas être une bonne solution pour préserver l'utilité des données. Pour résoudre ce problème, nous proposons pour préserver les propriétés importantes des graphes, telle que la distance, l'ajout de faux nœuds dans le graphe. Par exemple, si nous ajoutons simplement un faux nœud au graphe de la figure 3.2(a), nous

pouvons également générer un graphe 2-voisinage anonyme comme représenté sur la figure 3.3. Dans cette figure, les distances entre les nœuds du graphe original n'ont pas beaucoup changé.

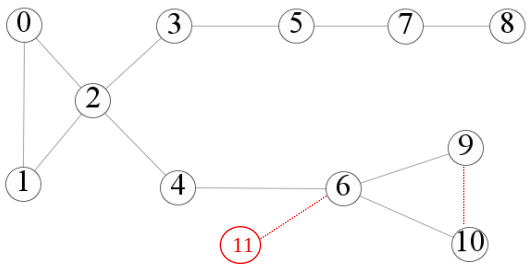


Figure 3.3 : un graphe 2-voisinage anonyme en ajoutant des faux nœuds

La solution basée sur l'ajout de faux nœuds semble préserver la propriété de la distance, notre contribution va s'articuler autour de cette idée.

4 Formulation du problème traité

Pour définir le problème de la protection des informations personnelles tout en publiant les données du réseau social contre l'attaque de voisinage, nous avons besoin de formuler les trois questions suivantes (comme montré sur la figure 3.4) :

- Premièrement, nous avons besoin d'identifier les informations privées à préserver ou à protéger.
- Deuxièmement, nous avons besoin de modéliser les connaissances de base qu'un adversaire peut utiliser pour compromettre la vie privée.
- Dernièrement, nous avons besoin de spécifier l'usage des données publiées du réseau social pour que la méthode d'anonymisation puisse essayer de retenir l'utilité des données autant que possible tout en préservant les informations privées.

L'objectif principal de notre travail est de protéger la vie privée des individus, représentés comme des sommets dans le graphe social. Considérons un graphe G = (V, E, L, *L*) et son graphe anonymisé publié G'= (V', E', L', *L*'). Pour un sommet u ∈ V, si un adversaire peut identifier un sommet u'∈ V', tel que la façon dont u se connecte à d'autres sommets dans G est similaire à la façon dont u' se connecte à d'autres sommets dans G', et diffère totalement de la façon dont d'autres sommets quelconques se connectent entre eux, alors la vie privée de u est divulguée. Par conséquent, les informations privées à préserver est d'empêcher tout sommet u ∈ V(G) d'être ré-identifié dans le graphe anonymisé G' avec une grande probabilité. Techniquement, Étant donné un entier positif k, G' préserve la vie privée des utilisateurs de G si chaque sommet u ∈ V(G) ne peut pas être ré-identifié dans G' avec une probabilité supérieure à 1/k.

Deuxièmement, les connaissances de base d'un adversaire seront des informations sur les voisinages de quelques sommets, c'est à dire, quels sont les voisins de la victime et comment ces voisins sont connectés. Dans notre cas nous considérons juste les voisins immédiats du sommet cible.

Un aspect très important de l'anonymisation des données du réseau social est comment les réseaux anonymisés sont devraient être utilisés, c-à-d l'objectif pour lequel le graphe anonymisé sera utilisé. Dans [54, 64, 78], le but était d'utiliser les réseaux sociaux pour répondre aux requêtes d'agrégation du réseau. Dans notre travail, nous nous intéressons à l'analyse des propriétés structurelles du graphe anonymisé résultant.

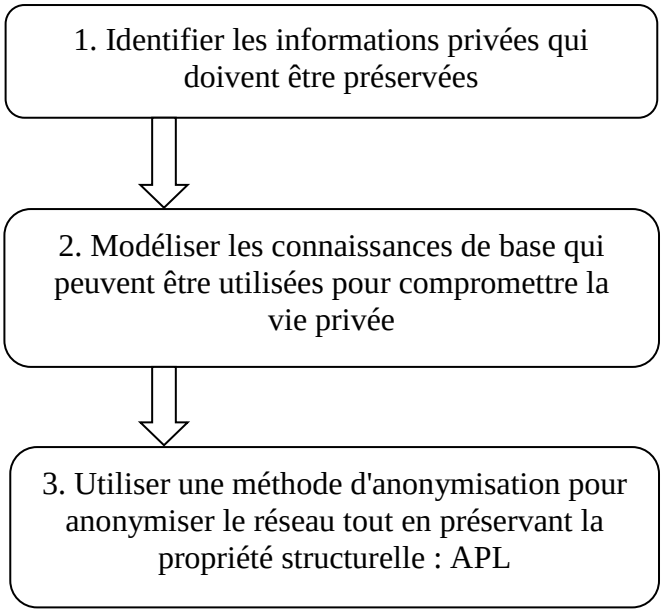


Figure 3.4 : Formulation du problème

Ainsi, nous définissons le problème traité comme suit :
Etant donné un graphe social G, nous voulons produire son graphe anonymisé G' tels que :
(1) G' est k-voisinage anonyme;
(2) Chaque sommet de G est anonymisé à un sommet dans G' et G' peut contenir de faux sommets;
(3) Chaque arête de G est retenue dans G' et
(4) G' peut être utilisé pour l'analyse des propriétés structurelles de façon aussi satisfaisante que possible.

5 Modélisation d'un réseau social

Généralement, un réseau social est modélisé comme un graphe simple G = (V, E, L, *L*), où V est un ensemble de sommets tel que chaque sommet correspond à un individu, E ⊆ V×V est un ensemble d'arêtes tel que chaque arête représente une relation sociale (amitié, intérêts communs, échanges financiers, etc.) entre deux individus. L est un ensemble de labels ou étiquettes, et une fonction d'étiquetage $L : V \rightarrow L$ qui attribue à chaque sommet un label. Pour un graphe G : V(G), E(G), L_G, et L_G sont, respectivement, l'ensemble des sommets, l'ensemble des arêtes, l'ensemble des labels, et la fonction d'étiquetage de G. Dans notre cas, nous supposons que les arêtes ne portent pas de labels. Les items dans l'ensemble de labels L forment une hiérarchie. Comme le montre l'exemple de la figure 3.5, si les professions sont utilisées comme labels de sommets dans un réseau social, L contient non seulement les professions spécifiques telles que dentiste, médecin généraliste, ophtalmologiste, enseignant de lycée, et enseignants de l'école primaire, mais aussi des catégories plus générales comme médecin, enseignant, et profession.

Nous supposons qu'il existe un symbole méta * ∈ L qui est la catégorie généralisant tous les labels (c'est la plus générale). Pour deux label l_1, 1_2 ∈ L, si l_1 est plus général que l_2, nous écrivons $l_1 < l_2$. Par exemple, médecin < ophtalmologiste. De plus, $l_1 \leq l_2$ si et seulement si $l_1 < l_2$ ou $l_1 = l_2$.

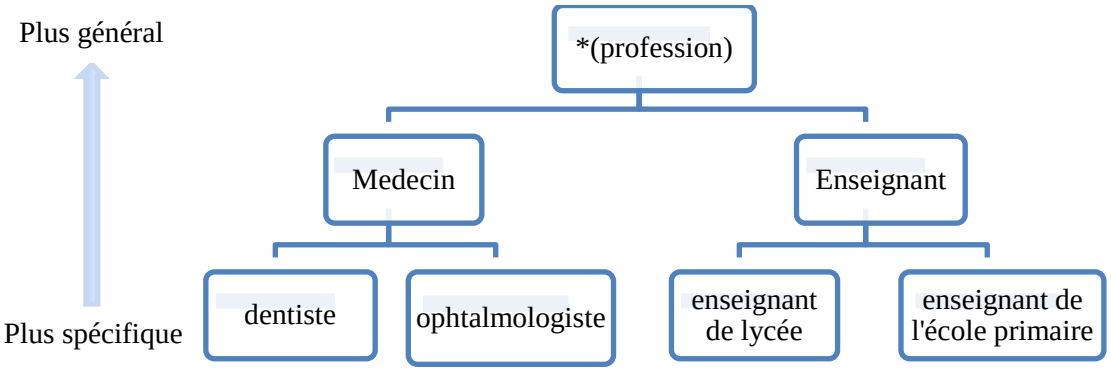


Figure 3.5: hiérarchie des labels

6 Quelques concepts de graphes sociaux

Avant de présenter notre approche d'anonymisation, il est nécessaire de définir quelques concepts de base utilisés dans notre travail.

6.1 Voisinage et d-voisinage d'un sommet

Dans un graphe social G, le voisinage d'un sommet $u \in V(G)$ est le sous-graphe induit par les voisins de u, notée $Neighbor_G(u) = G(V_u)$ où $V_u = \{v \mid (u, v) \in E(G)\}$ [54].
Le graphe d-voisinage d'un sommet u comprend tous les sommets qui sont dans la distance « d » du sommet u. [64]

6.2 Composante de voisinage

Dans un réseau social G, un sous-graphe C de G est une composante de voisinage de u ∈ V(G) si C est un sous-graphe connecté maximal dans $Neighbor_G(u)$. La figure 3.6 montre $Neighbor_G(u)$, le voisinage d'un sommet u, qui contient trois composantes de voisinage C_1, C_2 et C_3. Clairement, le voisinage d'un sommet peut être divisé en composantes de voisinage.

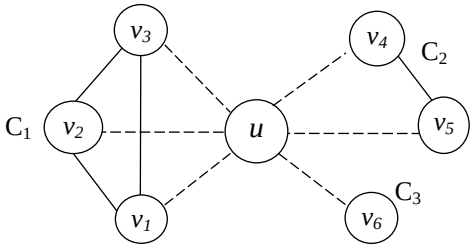


Figure 3.6 : Voisinage et composantes de voisinage (les arêtes pointillées sont juste pour illustration et ne sont pas dans le sous-graphe de voisinage) [54]

La table 1 résume les notations utilisées dans ce chapitre :

Symbole	Description
G	Le graphe initial modélisant un réseau social
V(G), E(G)	V : L'ensemble de sommets dans le graphe G, E: l'ensemble d'arêtes.
G'	Le graphe anonymisé du graphe social G
$Neighbor_G(u)$.	Voisinage du sommet u
$C_i(u)$	La composante numéro i dans le voisinage du sommet u
$\|V(C_i)\|$, $\|E(C_i)\|$	Le nombre de sommets et le nombre d'arêtes dans la composante C_i

Table 1 : Les notations utilisées

6.3 L'isomorphisme de graphe

Soient deux graphes : $G_1(V_1, E_1)$ et $G_2(V_2, E_2)$, où $|V_1| = |V_2|$, G_1 est isomorphe à G_2 si et seulement si il existe au moins une fonction bijective entre V_1 et V_2 :
$f: V_1 \rightarrow V_2$, telle que $\forall (u, v) \in E_1$, il existe une arête $((f(u), f(v)) \in E_2$.
Par exemple, les deux graphes ci-dessous (a) et (b) sur la figure 3.7 sont isomorphes. [80]

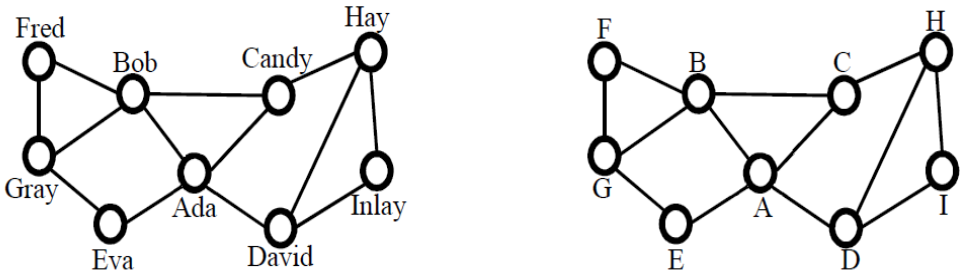


Figure 3.7: (a) Le réseau social original (b) le réseau avec des nœuds anonymes

6.4 L'isomorphisme de sous-graphe

Pour deux graphes $G_1 = (V_1, E_1)$ et $G_2 = (V_2, E_2)$, G_1 et G_2 sont sous-graphe isomorphes si G_1 contient un sous-graphe isomorphe à G_2. Comme le montre les graphes de (a) à (c) dans la figure 3.8, ils peuvent trouver les sous-graphes isomorphes correspondants dans la figure 3.7(b) [80].

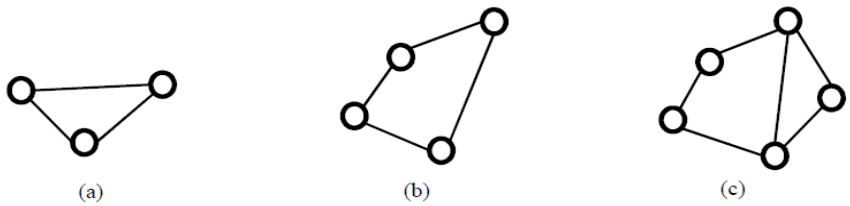


Figure 3.8 : Exemple d'isomorphisme de sous-graphe [80]

6.5 Le k-anonymat et l'anonymat de k-voisinage ou «k-neighborhood »

Etant donné un graphe social G(V,E), k un entier positif, et une connaissance de base b, G satisfait le « k-anonymat » contre b, si et seulement si pour chaque sommet v ∈V il y a au moins (k-1) autres sommets dans V partageant la propriété b.

Pour un sommet $u \in V(G)$, *u* est *k*-voisinage anonyme s'il y a au moins *(k - 1)* autre sommets $v_1,..., v_{k-1} \in V(G)$ tels que $Neighbor_{G'}(u)$, $Neighbor_{G'}(v_1)$, ..., $Neighbor_{G'}(v_{k-1})$ sont isomorphes.

Soit G' le réseau anonymisé de G, G' est *k*-voisinage anonyme si chaque sommet dans G est *k*-voisinage anonyme dans G'. Si G' est k-anonyme, alors avec des connaissances de base sur les voisinages, tout sommet dans G ne peut pas être ré-identifié dans G' avec une probabilité supérieure à 1/k. **[54]**

7 Utilité du graphe anonymisé et propriétés structurelles

Quand le graphe de réseau social est modifié, c'est un grand défi d'équilibrer entre la préservation de la vie privée et la perte de l'utilité des données. Dans le contexte de notre étude, nous nous intéressons aux mesures d'utilité reflétant les propriétés structurelles d'un graphe social G = (V, E), notamment l'APL. Ces caractéristiques sont généralement utilisées par des analystes, par exemple pour étudier l'influence, et les formes de communication dans les réseaux sociaux, faire du marketing viral ou étudier les modèles de propagation de l'information et de la maladie, etc. [42]. Dans cette section, nous présentons brièvement les propriétés structurelles des réseaux sociaux que nous considérons dans nos expériences et pour chacune nous donnons à titre d'exemple un type d'analyse qui se base sur cette propriété structurelle :

- La distance d(i, j) entre deux sommets i et j est la longueur du plus court chemin entre eux. Ou autrement dit le nombre minimal d'arêtes qu'on a besoin pour passer d'un nœud à l'autre.

- La distance entre toutes les paires de nœuds d'un graphe est mesurée par la longueur moyenne des plus courts chemins (Average shortest path length ou APL). APL est un concept dans la topologie de réseau qui est définie comme la moyenne sur la distance entre toutes les paires de nœuds. Certaines requêtes comme "le nœud le plus proche à un groupe de nœuds » sont liées à l'APL. Par exemple l'APL d'un graphe G est exprimée comme suit:

$$APL_G = \frac{2}{N(N-1)} \sum_{\forall\, i,j \in G} d(i,j)$$

  Où d(i,j) est la longueur du chemin le plus court entre les nœuds i et j, N est le nombre de nœuds dans le graphe.

- L'excentricité d'un nœud v est sa distance maximale à tous les autres nœuds, et est définie par : [42]

$$\varepsilon(v) = \max \{d(v, w) \mid w \in V\}.$$

- Le rayon d'un graphe est l'excentricité minimale de ses nœuds, c'est-à-dire la plus petite distance à laquelle puisse se trouver un nœud de tous les autres, et définie par :

$$\text{Rayon}(G) = \min\{\varepsilon(v) \mid v \in V\}.$$

Le centre d'un graphe est formé de l'ensemble de ses nœuds d'excentricité minimale. Comme exemple d'utilisation pratique du rayon d'un graphe social dans l'épidémiologie, imaginons qu'une maladie se propage d'un individu à ces voisins au bout d'un jour. Soit j le jour où un individu est infecté, au jour (j + n) si n < rayon(G) alors on est sûr qu'il reste au moins (rayon(G) - n) individus non encore infectés et on peut donc encore réagir. Un autre exemple, la propagation rapide d'information, ou de rumeur peut être mesurée. Ceci pourrait être intéressant dans le cadre de marketing [42].

- Le diamètre d'un graphe est l'excentricité maximale de tous les nœuds du graphe, autrement dit c'est la plus grande distance possible qui puisse exister entre deux de ses sommets, et est définie par :

$$\textit{Diametre}(G) = \max\{\varepsilon(v) \mid v \in N\}.$$

Dans l'étude des grands réseaux d'interactions comme les réseaux sociaux, il est souvent fait référence à un petit diamètre pour décrire l'observation d'une petite distance moyenne. Dans ce contexte, nous citons le problème du petit monde (small world) où les expériences sondaient la distribution des longueurs de chemins dans un réseau de connaissance en demandant aux participants de passer une lettre à une de leurs premières connaissances dans une tentative de se rendre à un individu cible. Le résultat obtenu était, il suffit, en moyenne, six nœuds intermédiaires pour faire arriver une lettre à un individu cible [20]. Une telle expérience a permis d'établir la théorie de « six degrés de séparation » [42].

- La densité d'un graphe G est le rapport entre le nombre d'arêtes divisé par le nombre d'arêtes possibles, et est définie par :

$$\text{Densite}(G) = \frac{|E|}{\binom{n}{2}} = \frac{2|E|}{n(n-1)}$$

Tel que n est le nombre de nœuds du graphe G, et |E| est le nombre d'arêtes. Une densité élevée est le reflet d'un grand nombre d'arêtes dans un graphe social [42].

8 Proposition d'une nouvelle approche d'anonymisation

Un défi majeur dans l'anonymisation d'un réseau social, est que le changement des labels des sommets et l'ajout des arêtes ainsi que des faux sommets peuvent affecter les voisinages d'autres sommets ainsi que les propriétés du réseau. Il est bien reconnu que les deux propriétés suivantes sont souvent retenues dans les réseaux sociaux. Ces propriétés nous aident dans la conception de notre méthode d'anonymisation.

Propriété 1*: « la distribution des degrés des sommets suit une loi de puissance »* : la distribution des degrés des sommets dans un grand réseau social suit souvent la loi de puissance [21]. Ces distributions de degré ont été identifiées dans divers réseaux sociaux, incluant Internet, les réseaux biologiques et les réseaux de co-auteur.

Propriété 2: *«le phénomène de petit-monde »* [20]. Il est également populairement connu sous « six degrés de séparation », qui précise que les grands réseaux sociaux en pratique ont souvent étonnamment des petits diamètres moyens.

Notre méthode d'anonymisation de réseau social traite les sommets dans l'ordre décroissant de degré, et utilise les deux propriétés ci-dessus.

Le k-anonymat exige que chaque sommet $u \in V(G)$ soit groupé avec au moins *(k-1)* autres sommets tels que leurs voisinages anonymisés soient isomorphes. Pour un groupe *S* de sommets ayant des voisinages anonymisés isomorphes, tous les sommets dans S ont le même degré. Puisque les degrés des sommets dans un grand réseau social suivent une distribution en loi de puissance, seulement un nombre restreint de sommets ont un degré élevé. Traiter d'abord les sommets de degré élevé peut limiter la perte d'informations relatives à ces sommets. Il y a souvent beaucoup de sommets de degré faible. Il est relativement facile d'anonymiser ces sommets de degré faible et maintenir l'utilité du graphe. En outre, comme sera montré plus loin, les sommets de degré faible peuvent être utilisés pour anonymiser les sommets de degré élevé et ne pas trop affecter le diamètre du réseau.

La technique d'anonymisation proposée par Zhou et Pei [54] consiste à ajouter des liens entre les différents sommets du graphe pour satisfaire la condition de « k-voisinage » c.à.d. tout individu dans le réseau social anonymisé ne peut pas être ré-identifié correctement avec une probabilité supérieure à 1/k. Bien que cette technique d'anonymisation produise un niveau élevé (proportionnel au nombre k de la condition de k-anonymat) de garantie en termes de protection de la vie privée des individus présents dans le graphe social, l'utilité d'un tel graphe social publié n'atteint pas un niveau acceptable du point de vue des propriétés structurelles.
En résumé, les solutions basées sur l'ajout de liens présentent une limitation majeure, à savoir :

> *Le risque de modifier la propriété de distance sensiblement en reliant deux nœuds lointains qui appartiennent à deux communautés différentes. Par conséquent, toute analyse sur les données anonymisées concernant les différentes propriétés structurelles pourrait obtenir des conclusions erronées ou non valides.*

Ainsi, compter uniquement sur l'ajout de liens ne peut pas être une bonne solution pour préserver l'utilité des données.
Dans ce travail de recherche, l'idée consiste à développer une nouvelle technique d'anonymisation de graphe social qui ne se base pas seulement sur l'ajout de liens mais aussi sur l'ajout de faux nœuds dans le but d'atteindre un compromis entre la préservation de la vie privée et l'utilité résultante du graphe anonymisé. La principale différence entre notre travail et les travaux antérieurs [54, 64, 78,77] est que nous garantissons que le graphe publié préserve une utilité importante, à savoir « la longueur des plus courts chemins ». Ceci se traduit par la limitation des distorsions de distance entre les sommets du graphe anonymisé et les sommets du graphe original. Ce qui permettra de préserver autant que possible la valeur de « la longueur moyenne de chemins les plus courts » ou « APL », par l'ajout de faux nœuds dans le graphe. L'idée d'ajout de faux nœuds est basée sur l'observation clé suivante :

La plupart des réseaux sociaux satisfont la distribution en loi de puissance [21], c.-à-d., il existe un grand nombre de sommets de degré bas dans le graphe social qui pourraient être utilisés pour cacher les faux nœuds ajoutés d'être identifiés. En insérant soigneusement les faux nœuds, certaines propriétés des graphes pourraient être mieux préservées par rapport à la méthode d'ajout de liens pure.

Notre contribution majeure consiste à proposer un nouvel algorithme efficace d'anonymisation de réseau social qu'on l'a appelé « AnonSN », qui préserve non seulement la vie privée des individus présents dans le graphe social publié, en prévenant qu'un attaquant puisse identifier un utilisateur en utilisant la connaissance de voisinage, mais aussi qui maintient autant que possible les différentes propriétés structurelles du graphe original, notamment la distance. Cet algorithme repose sur la combinaison du principe d'*« ajout de liens »* et celui d'« *ajout de faux nœuds* ».

Notre algorithme qui sera présenté dans la section 8.2, fait partie des algorithmes d'anonymisation d'un graphe social par modification. Il est également basé sur le modèle « k-voisinage », il assure que pour chaque nœud du graphe, il existe au moins (k-1) nœuds ayant des voisinages isomorphes, autrement dit, l'adversaire ne peut pas distinguer un nœud parmi k nœuds.

L'approche d'anonymisation proposée garantit que, pour toute modification apportée au graphe original, la propriété de distance moyenne entre les sommets impliqués est aussi proche que possible à celle dans le graphe original. Nous avons proposé également une nouvelle formule de calcul du coût d'anonymisation. En résumé, nous avons apporté les principales contributions suivantes:

1. Proposition d'une nouvelle formule de calcul du coût d'anonymisation pour déterminer les voisinages des sommets qui peuvent êtres anonymisés ensemble.
2. Proposition d'une nouvelle approche d'anonymisation basée sur l'ajout de faux nœuds en plus de l'ajout de liens.
3. Comparaison des performances de l'approche proposée d'ajout de faux nœuds par rapport à l'approche de Zhou et Pei selon la préservation de l'APL.

Afin de maintenir l'utilité du graphe à publier, il est nécessaire d'ajouter le moins possible d'arêtes ainsi que de faux sommets. L'architecture de notre approche d'anonymisation est illustrée dans la figure 3.9 ci-dessous :

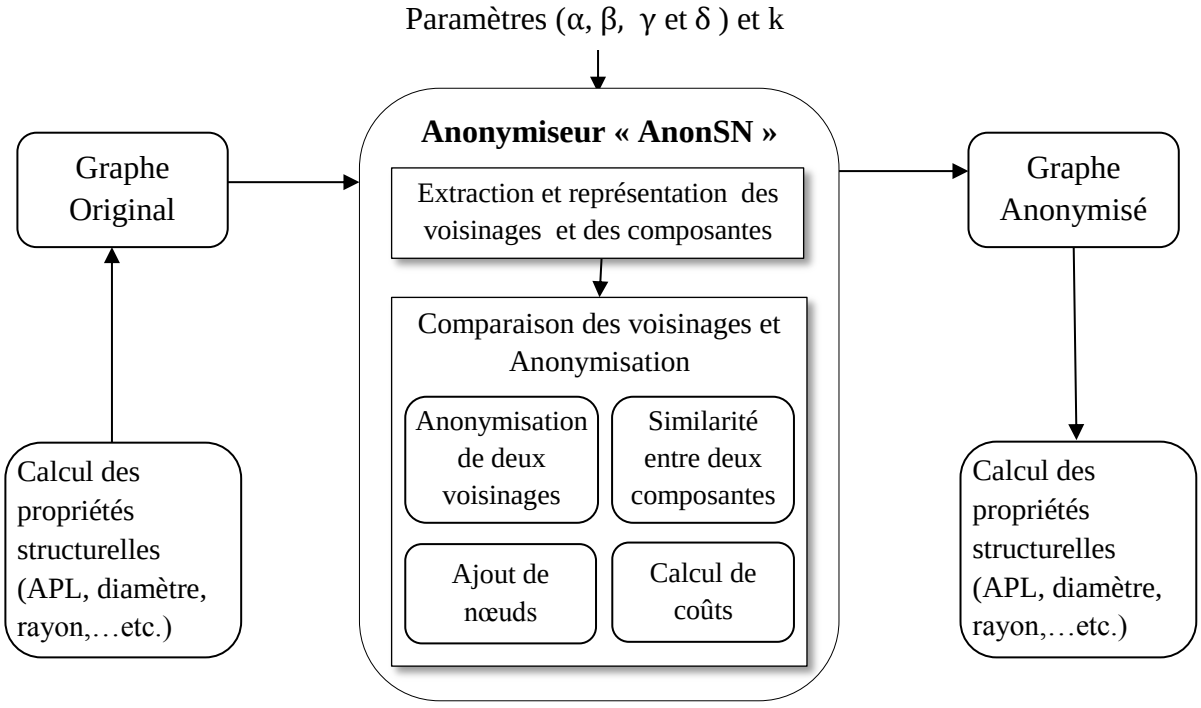


Figure 3.9 : Architecture de l'approche d'anonymisation

On part d'un graphe G qui n'est pas anonymisé, comme celui déjà présenté dans la figure 3.2(a). Ce graphe a certaines propriétés structurelles calculées dans le module «Calcul des propriétés structurelles », on le fait passer par le module d'anonymisation « Anonymiseur » ou « AnonSN », on obtient ainsi un graphe anonymisé avec d'autres propriétés structurelles.

Le module «Calcul des propriétés structurelles » reçoit en entrée un graphe quelconque (anonymisé ou non anonymisé), et nous produit comme résultat les valeurs de toutes les propriétés structurelles qu'on veut préserver telles que : APL, le diamètre, le rayon, …etc.

Le module d'anonymisation « L'anonymiseur » reçoit en entrée le graphe G non anonymisé modélisant un réseau social, un paramètre d'anonymisation k, et trois paramètres α, β, γ et δ qui servent à calculer le coût d'anonymisation, pour produire en sortie un graphe satisfaisant la condition de k-anonymat de sorte que pour chaque sommet du graphe il y'a au moins (k-1) autres sommets tels que leurs voisinages anonymisés sont isomorphes. Et ceci selon les deux étapes illustrées dans la figure 3.9.

8.1 Extraction et représentation des voisinages et des composantes de voisinages

Les voisinages de tous les sommets dans le graphe G sont extraits et les différentes composantes sont séparées. Pour faciliter les comparaisons entre les voisinages des différents sommets, y compris les tests d'isomorphisme qui seront fréquemment effectués dans l'anonymisation, nous avons choisi les matrices d'adjacence pour représenter les différentes composantes de voisinage, tel que :

$$M[i,j]=\begin{cases}1 & \text{si } (i,j) \in E \\ 0 & sinon\end{cases}$$

Reprenant l'exemple de voisinage de « Walid » de la figure 3.2(c), les composantes de voisinage de « Walid » et les matrices d'adjacence qui les représentent sont illustrées dans la figure 3.10 ci-dessous :

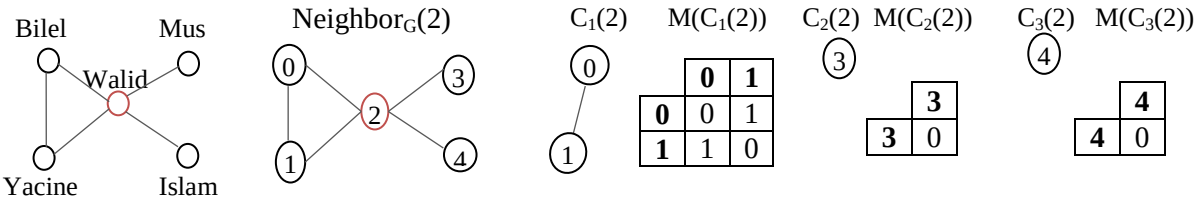


Figure 3.10 : Voisinage et composantes de voisinage de « Walid »

Notons que Zhou et Pei [54] ont utilisé un codage DFS pour représenter les composantes de voisinage. Dans un travail ultérieur, Tripathy et al [64] ont proposé les matrices d'adjacence comme technique de codage et calcul de similarité entre les différents voisinages (au lieu les codes DFS) dont ils ont prouvé leur efficacité ainsi que leur complexité minimale par rapport aux codes DFS.

L'algorithme 1 représente la procédure d'extraction et de représentation des voisinages et des composantes de voisinages sous forme de matrices d'adjacence.

Algorithme1 : Algorithme d'extraction et de représentation des voisinages et des composantes des voisinages

Entrée: *M(G):* la matrice d'adjacence d'un graphe de réseau social $G = (V, E)$
Sortie: *W*: ensemble des voisinages de tous les sommets $v_i \in V$ tel que chaque voisinage contient les différentes composantes représentées sous forme de matrices d'adjacence;
VertexList : la liste contenant tous les sommets v_i selon l'ordre décroissant de la taille de leurs voisinages ;

Début

W←∅;

Pour tout $v_i \in V(G)$ ***faire***

$Neighbor_G(v_i) \leftarrow \emptyset$;
voisins ← ∅

//Construire la liste des voisins du sommet v_i
pour chaque u ∈ M(G) ***faire***
si (M[v_i][u] ≠ 0) **alors**
voisins ← *u*
finsi
fin pour

// Construire la liste des composantes de voisinage du sommet v_i et leurs matrices d'adjacence
tant que (*voisins* ≠ ∅) ***faire***
head ← *voisins.head* // Le premier sommet de la liste *« voisins»*
Supprimer head de la liste *voisins* *// pour ne pas le recalculer*
pour tout *u* ∈ *voisins* ***faire***
si (M[head][u] ≠ 0) ***alors*** // head et u sont reliés => ils appartiennent à la même composante
com ← *u*
head←*u* // réinitialiser head par le nouveau somet pour déduire les autres sommets reliés dans la même composante
Supprimer *u* de la liste *voisins*
fin si
fin pour
Construire la matrice *M(com)* de la composante com
Trier *M(com)* par degré et par label
$Neighbor_G(v_i) \leftarrow M(com)$;
fin tant que
$W \leftarrow Neighbor_G(v_i)$;

Fin pour

Trier W par ordre décroissant de la taille des différents voisinages, et insérer chaque $v_i \in V(G)$ dans « *VertexList* » selon cet ordre.

//Comparer 2 voisinages
Pour deux sommets $u, v \in V(G)$ ***faire***
Si ($|V(Neighbor_G(u))| < |V(Neighbor_G(v))|$) ou ($|V(Neighbor_G(u))| = |V(Neighbor_G(v))|$ et $|E(Neighbor_G(u))| < |E(Neighbor_G(v))|$) ***alors*** *v* précède *u* dans la liste « *VertexList* » ;
Sinon
si ($|V(Neighbor_G(u))| = |V(Neighbor_G(v))|$ et $|E(Neighbor_G(u))| = |E(Neighbor_G(v))|$ ***alors***
ordonner u et v arbitrairement ;
fin si
Fin si
Fin pour

Retourner (*W,VertexList) ;*

Fin

8.2 Comparaison des voisinages et anonymisation

Dans cette étape, nous organisons les sommets en groupes (avec des tailles d'au moins k), le facteur du «Coût d'anonymisation», également connu comme « la mesure de qualité d'anonymisation » est calculé pour chaque paire de sommets. Les sommets avec le minimum de différence du coût peuvent être groupés ensemble pour l'anonymisation. Ensuite, nous anonymisons les voisinages des sommets dans le même groupe en se basant sur l'ajout d'arêtes et l'ajout de faux nœuds dans le graphe original tout en préservant la distance moyenne entre les différents sommets. La procédure d'anonymisation suit les étapes suivantes :

- D'abord, tous les sommets du graphe sont considérés non anonymes et donc marqués « unaonymized ».
- Puis nous maintenons une liste « vertexList » des sommets non anonymisés suivant l'ordre décroissant de la taille de leurs voisinages. Pour deux sommets u et $v \in V(G)$, si $|V(Neighbor_G(u))| < |V(Neighbor_G(v))|$, ou $|V(Neighbor_G(u))| = |V(Neighbor_G(v))|$ et $|E(Neighbor_G(u))| < |E(Neighbor_G(v))|$ alors v précède u dans la liste « vertexList ». Si leurs voisinages ont le même nombre de sommets et d'arêtes, ils peuvent être ordonnés arbitrairement.
- Ensuite, itérativement, nous choisissons le premier sommet « head » dans la liste « vertexList ». Le coût d'anonymisation de « head » avec tout autre sommet dans « vertexList » est calculé en utilisant la méthode d'anonymisation de deux voisinages comme suit :
    a. Soient u, v∈ V(G), u et v ont des voisinages similaires, alors les labels sont généralisés ou laissés inchangés, de sorte que les voisinages de u et v soient isomorphes, et les labels des sommets sont les mêmes dans les deux voisinages.
    b. Si les voisinages ne sont pas similaires, le coût est calculé et la paire de sommets avec coût minimal est considérée.
    c. Des arêtes et des sommets sont ajoutés pour les rendre similaires.
    d. Le processus de l'étape (a) est appliqué sur la paire de sommets.

- Si le nombre de sommets non anonymisés dans « vertexList » est au moins 2k -1, nous sélectionnons les premiers $(k-1)$ sommets qu'on appelle « CandidateSet », de la liste « vertexList » qui offrent un plus petit coût d'anonymisation.
- Le sommet « head » et les sommets dans CandidateSet = $\{u_1,...,u_m\}$ sont anonymisés à tour de rôle selon la méthode d'anonymisation de deux voisinages. L'anonymisation de head et u_l est directe. Après que ces deux sommets sont anonymisés, leurs voisinages deviennent identiques. Quand on les anonymise en respectant u_2, tout changement (par exemple, l'ajout d'une arête ou d'un nœud) dans le voisinage de head (qui était déjà anonymisé avec u_1) sera aussi appliqué à u_1, de sorte que les voisinages de head, u_l et u_2 soient isomorphes. Le processus se poursuit jusqu'à ce que les voisinages de « head » et $u_1,\ldots,u_m$ deviennent isomorphes.
- Durant la procédure d'anonymisation d'un groupe de sommets, des changements peuvent affecter certains sommets v qui sont déjà marqués "anonymized" dans un autre groupe (par exemple, l'ajout d'une arête entre un sommet anonymisé et un sommet à anonymiser). Afin de maintenir le k-anonymat pour ces sommets, nous appliquons les mêmes changements à chacun des autres $(k-1)$ sommets ayant des voisinages isomorphes à v. Une fois que ces k sommets sont modifiés, ils sont marqués comme « unanonymized » et réinsérés dans « vertexList ».

- Lorsque le nombre de sommets non anonymisé dans « vertexList » est inférieur à 2k, pour satisfaire le k-anonymat, les sommets restants dans « vertexList » doivent être considérés ensemble dans l'anonymisation. Ils sont tous ajoutés à l'ensemble «CandidateSet».
- L'algorithme d'anonymisation continue jusqu'à ce que tous les sommets du graphe soient marqués "anonymized". L'algorithme 2 représente la procédure d'anonymisation du graphe social.

Algorithme 2: Algorithme d'anonymisation d'un réseau social pour atteindre le *k-anonymat*

Entrée : un graphe social $G = (V, E)$, le paramètre d'anonymat k, les paramètres de la fonction Coût $\alpha, \beta, \gamma, \delta$
Sortie : un graphe anonymisé *G' « k-voisinage »* ;
Initialisation: $G' \leftarrow G$, $CandidateSet \leftarrow \emptyset$;

Début

Supprimer les identifiants des sommets ; // anonymisation naïve
W← les voisinages de tous les sommets $v_i \in V(G)$; *// voisinages extraits selon l'algorithme 1*
VertexList ← la liste contenant tous les sommets v_i selon l'ordre décroissant de la taille de leurs voisinages ;

Pour tout $v_i \in V(G)$ **faire**
Marquer v_i *comme* "unanonymized";
Fin pour

Tant que *VertexList* $\neq \emptyset$ **faire**

head ← *VertexList.head*() // Le premier sommet de la liste « *VertexList* » qui a le degré le plus élevé
Supprimer *head* de *VertexList*

Pour chaque $v_i \in$ *VertexList* ***faire***
Calculer *Cost (*head, v_i, $\alpha, \beta, \gamma, \delta$*)* // En utilisant la méthode de calcul de coût d'anonymisation de deux sommets
Fin pour

Si* taille(VertexList)*** $\geq 2k - 1$ ***alors***
CandidateSet ← les premiers $(k - 1)$ sommets ayant un cout minimal // i.e les (k-1) sommets ayant les voisinages les plus similaires au voisinage de head
Sinon *CandidateSet* ←les sommets non anonymisés restants dans *VertexList* ;
Fin Si

CandidateSet= $\{u_1, \ldots, u_m\}$
Anonymiser *Neighbor*(*head*) et *Neighbor*(u_1) *comme expliqué dans la section 8.2.2*

Pour $j = 2$ à m ***faire***
Anonymiser récursivment *Neighbor*(u_j) et {*Neighbor*(*head*), *Neighbor*(u_1), . . . ,*Neighbor*(u_{j-1})} comme expliqué dans la section 8.2.2
Marquer u_j comme "anonymized";
Mettre à jour *VertexList*;
Fin pour

Substituer les voisinages des nœuds dans le graphe original par les voisinages isomorphes ;

Fin Tant que

Retourner *G'*

Fin

La formule de calcul du coût d'anonymisation proposée, la méthode d'anonymisation de deux voisinages, la méthode de vérification de la similarité et d'anonymisation de deux composantes ainsi que la méthode d'ajout de nœuds seront expliquées dans les sections suivantes.

8.2.1 Mesure de la qualité de l'anonymisation « Coût d'anonymisation »

L'objectif principal d'algorithmes d'anonymisation de réseau social est de développer des heuristiques efficaces pour assurer un équilibre entre la préservation de la structure du graphe original et la vie privée des individus. Durant l'anonymisation, l'information exacte dans le graphe original G est modifiée (ou plus précisément, perdue). En outre, il n'est pas clair comment quantifier la diminution de l'utilité lors de l'anonymisation d'un graphe. Une façon de mesurer la différence entre les graphes originaux et les graphes anonymisés est de compter le nombre de nœuds et d'arêtes qui ont été ajoutés ou supprimés. Toutefois, cela peut ne pas être toujours une quantification précise de l'effet de l'anonymisation sur l'utilité. La force d'un algorithme d'anonymisation peut être mesurée en termes de *perte de l'information*. Pour préserver l'utilité du graphe anonymisé, une propriété désirée est de perdre le moins possible d'information.

Dans notre modèle d'anonymisation, nous avons proposé une nouvelle formule de calcul de coût d'anonymisation. Il y a trois façons pour anonymiser les voisinages des sommets : *« généraliser les labels de sommet », « ajouter des arêtes » et « ajouter des faux nœuds »*. Chacune des trois méthodes conduit à une certaine perte d'information.

- La perte d'information due à la généralisation des labels de sommets peut être mesurée par la pénalité normalisée de la certitude ou « the normalized certainty penalty » ou NCP. Soit *u* un sommet de label l_1 (par exemple l_1= « pédiatre »), tel que l_1 est un nœud feuille dans la hiérarchie des labels, c.-à-d. l_1 n'a aucun label descendant. Supposons que l_1 est généralisé en l_2 pour *u* où $l_2 < l_1$ (par exemple l_2= «médecin »). Notons $size(l_2)$ le nombre de descendants de l_2 qui sont des feuilles dans la hiérarchie des labels, et $size(*)$ le nombre total des feuilles dans la hiérarchie des labels. La pénalité normalisée de la certitude de l_2 est définie par:

$$\mathrm{NCP}(l_2) = \frac{size(l_2)}{size(*)}$$

- La perte d'information due à l'ajout des arêtes peut être mesurée par *le nombre total d'arêtes ajoutées* et *le nombre de sommets* qui n'appartiennent pas au voisinage du sommet cible et sont reliés au voisinage anonymisé dans le but de l'anonymisation.

- La perte d'information due à l'ajout de faux sommets peut être mesurée par *le nombre total de faux sommets ajoutés* au voisinage du sommet cible.

Soit G = (V, E) un graphe social, et G' = (V', E') sa version anonymisée. Considérons deux sommets *u*, *v* ∈ V(G). Supposons que leurs voisinages $Neighbor_G(u)$ et $Neighbor_G(v)$ sont généralisés à $Neighbor_{G'}(u)$ *et* $Neighbor_{G'}(v)$ tels que $Neighbor_{G'}(u)$ et $Neighbor_{G'}(v)$ sont isomorphes. Soit H = $Neighbor_G(u) \cup Neighbor_G(v)$ et H' = $Neighbor_{G'}(u) \cup Neighbor_{G'}(v)$. Soient nb: le nombre de sommets existants ajoutés, et nbf: le nombre de faux sommets ajoutés. Le coût d'anonymisation est défini comme suit :

$$\text{Cost (u,v)} = \alpha \cdot \sum_{v' \epsilon H'} NCP(v') + \beta \cdot |\{(v_1, v_2) \ / \ (v_1, v_2) \notin E(H),\ (v_1, v_2) \in E(H')\}| + \gamma \cdot (nb) + \delta \cdot (nbf)$$

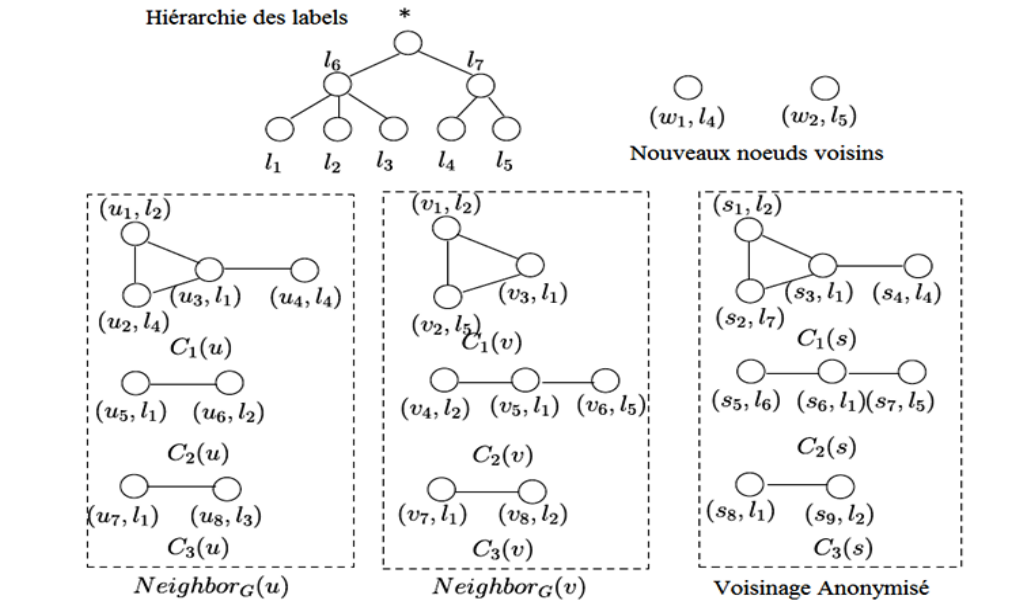
Où α, β, γ et δ sont des poids spécifiés par l'utilisateur lors de l'anonymisation du graphe, et permettront de privilégier une technique à une autre. Littéralement, le coût est constitué de quatre parties : la première partie représente la pénalité normalisée de la certitude mesurant la perte d'information due à la généralisation des labels de sommets. La seconde partie mesure la perte d'information due à l'ajout des arêtes. La troisième partie compte le nombre de sommets existants dans le graphe qui sont reliés aux voisinages anonymisés pour atteindre le k-anonymat. Et la dernière partie compte le nombre de faux sommets ajoutés aux voisinages des sommets u et v au lieu de certains sommets existants.

Le coût d'anonymisation des deux sommets u et v mesure la similarité entre $Neighbor_G(u)$ et $Neighbor_G(v)$. Plus le coût d'anonymisation est faible plus les deux voisinages sont similaires. Par conséquent, l'anonymisation des voisinages similaires peut conduire à une faible perte de l'information et une grande similarité entre le réseau social original et celui anonymisé.

8.2.2 L'Anonymisation de deux voisinages

Soient les deux sommets u et v dont les voisinages $Neighbor_G(u)$ et $Neighbor_G(v)$ et la hiérarchie des labels sont représentés sur la Figure 3.11. Les composantes de chaque voisinage sont ordonnées dans l'ordre décroissant de leur nombre de sommets, et chaque sommet est représenté sous la forme *(id, label).* Les matrices d'adjacence pour toutes les composantes sont comparées pour la similarité dans l'ordre suivant :
Pour commencer, nous recherchons toutes les correspondances parfaites entre les composantes de voisinage dans $Neighbor_G(u)$ et $Neighbor_G(v)$. Deux composantes correspondent parfaitement si elles ont la même matrice d'adjacence ainsi que les mêmes labels. Ces correspondances parfaites sont marquées comme « matched ». Dans l'exemple illustré dans la figure 3.11, la composante de voisinage $C_2(u) \in Neighbor_G(u)$ correspond parfaitement à $C_3(v) \in Neighbor_G(v)$ (ont les mêmes matrices d'adjacence ainsi que les mêmes labels). La composante de voisinage anonymisée correspondante est C_3 (s).

Pour les composantes qui ne correspondent pas, l'algorithme d'anonymisation essaye d'apparier les composantes similaires et de les anonymiser. La similarité entre deux composantes est basée sur le coût d'anonymisation. Pour calculer la similarité entre deux composantes, nous comparons les matrices d'adjacence et les labels des deux composantes et nous calculons le coût d'anonymisation. La méthode de vérification de similarité entre deux composantes sera détaillée dans la section prochaine.



	u_3	u_1	u_2	u_4
u_3	0	1	1	1
u_1	1	0	1	0
u_2	1	1	0	0
u_4	1	0	0	0

$M(C_1(u))$

	u_5	u_6
u_5	0	1
u_6	1	0

$M(C_2(u))$

	u_7	u_8
u_7	0	1
u_8	1	0

$M(C_3(u))$

Les matrices d'adjacences des composantes de $Neighbor_G(u)$

	v_1	v_2	v_3
v_1	0	1	1
v_2	1	0	1
v_3	1	1	0

$M(C_1(v))$

	v_5	v_4	v_6
v_5	0	1	1
v_4	1	0	0
v_6	1	0	0

$M(C_2(v))$

	v_7	v_8
v_7	0	1
v_8	1	0

$M(C_3(v))$

Les matrices d'adjacences des composantes de $Neighbor_G(v)$

	s_3	s_1	s_2	s_4
s_3	0	1	1	1
s_1	1	0	1	0
s_2	1	1	0	0
s_4	1	0	0	0

$M(C_1(s))$

	s_6	s_7	s_5
s_6	0	1	1
s_7	1	0	0
s_5	1	0	0

$M(C_2(s))$

	s_8	s_9
s_8	0	1
s_9	1	0

$M(C_3(s))$

Les matrices d'adjacences des composantes anonymisées

Figure 3.11 : Exemple d'anonymisation de deux voisinages.

Nous commençons par la composante ayant le plus grand nombre de sommets. Nous essayons de trouver une composante dans l'autre voisinage qui lui corresponde le mieux selon le coût d'anonymisation en calculant le nombre de sommets et d'arêtes à ajouter et la pénalité normalisée de la certitude de la généralisation des labels dans la hiérarchie de labels. Nous choisissons celle avec le coût d'anonymisation minimal. S'il y a plusieurs composantes avec le même coût, alors la composante est choisie aléatoirement. Ensuite, nous marquons la paire de composantes comme « matched ».

Considérons les composantes $C_1(u)$ et $C_1(v)$ de la figure 3.11. Les matrices de ces deux composantes ne sont pas identiques, Ainsi, nous devons trouver un sommet $w_1 \in V(G)$ qui n'est ni dans $C_1(v)$ ni dans $C_1(u)$, et l'ajouter à $C_1(v)$, ou bien générer un faux sommet et l'ajouter à $C_1(v)$ et à $V(G)$, de sorte que $C_1(u)$ et $C_1(v)$ soient isomorphes, leurs matrices soient identiques et la distance moyenne entre le sommet v et le reste des sommets soit préservée, c.-à-d. plus proche à la moyenne originale avant que le sommet ne soit ajouté. Les critères de choix entre l'ajout d'un sommet existant et un faux sommet seront détaillés dans la section 8.2.4.

Dans notre exemple, supposons que nous pouvons trouver un sommet existant non anonymisé (w_1, l_4) à ajouter dans $C_1(v)$, le coût d'anonymisation de $C_l(v)$ et $C_1(u)$ est :

$$\alpha.\sum_{v' \in V(C_1(u)) \sqcup V(C_1(v))} NCP(L(v')) + \beta.1 + \gamma.1 + \delta.0 = = \alpha.\frac{4}{5} + \beta + \gamma$$

En résumé, en se basant sur la similarité des composantes, nous pouvons apparier les composantes similaires. Nous commençons par la composante avec le nombre de sommets le plus élevé. Cette composante est appariée avec la composante la plus similaire dans l'autre voisinage. Les deux composantes appariées sont anonymisées et marquées «matched». Le matching continue jusqu'à ce que toutes les composantes dans un voisinage soient marquées « matched ».

S'il y a des composantes restantes dans l'autre voisinage disons dans $Neighbor_G(u)$, nous utilisons d'autres sommets de $V(G)$ qui ne sont pas dans $Neighbor_G(v)$ ou des faux sommets pour construire une composante et l'ajouter à $Neighbor_G(v)$ pour construire le matching et l'anonymisation. Les sommets à ajouter sont sélectionnés selon les mêmes critères de sélection des sommets à ajouter pour correspondre deux composantes.

Nous anonymisons chaque paire de composantes de voisinage appariée. Par conséquent les deux voisinages sont anonymisés. Par exemple, sur la figure 3.11, l'algorithme fait correspondre les composantes $C_1(u)$ et $C_1(v)$, $C_2(v)$ et $C_3(u)$ à leur tour. Ainsi, deux sommets w_1 et w_2 de V(G) doivent être ajoutés dans les composantes $C_1(v)$ et $C_3(u)$, respectivement.

Notons qu'une fois que deux voisinages sont anonymisés, les voisinages de certains sommets peuvent être changés. Nous avons besoin de mettre à jour les voisinages de ces derniers.

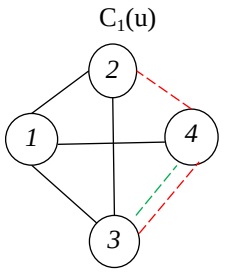
8.2.3 Méthode de vérification de la similarité et d'anonymisation de deux composantes

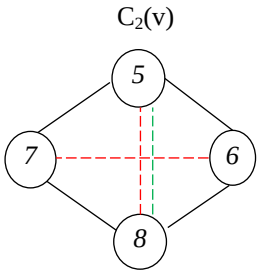
Le problème général d'isomorphisme de graphe qui détermine si deux graphes sont isomorphes est NP-difficile [54]. Pour déterminer l'isomorphisme des graphes de voisinage de deux sommets, des techniques de codage des sous-graphes de voisinage sont proposées dans [54] et [64] de sorte que l'isomorphisme de deux voisinages puisse être déterminé par le codage correspondant. Le codage par arbre DFS a été utilisé par Zhou et Pei dans [54] pour coder les différentes composantes de voisinage. Cependant, une technique plus efficace a été développée par Tripathy et al [64] utilisant les matrices d'adjacence qui a été prouvé moins complexe par rapport les arbres DFS.

Les graphes de voisinage de tous les sommets sont séparés en leurs composantes et sont représentés sous forme de matrices d'adjacence. Nous expliquons dans cette section, comment ces composantes sont comparées pour vérifier la similarité entre elles.

Deux composantes sont isomorphes s'il est possible d'ordonner leurs ensembles de sommets respectifs de sorte que leurs matrices d'adjacence soient identiques et leurs labels soient les mêmes. La matrice d'adjacence est construite dans l'ordre décroissant des degrés de sommets et de leur label dans la composante. Quand deux ou plusieurs sommets ont le même degré, le tri se fait en fonction de l'ordre décroissant des labels. Deux composantes avec la même séquence de degrés et ayant les mêmes matrices d'adjacence sont isomorphes selon leur structure. Ensuite, si les labels correspondent aussi, alors elles sont isomorphes. Sinon, les labels seront généralisés à leur label parent dans la hiérarchie des labels.

Pour deux composantes avec le même nombre de sommets, si leurs matrices ne sont pas identiques, nous déterminerons toutes les combinaisons possibles entre les sommets construisant ces matrices et ceci dans le but de réduire autant que possible le nombre d'arêtes ajoutées. Notons qu'une permutation entre 2 sommets n'est possible que s'ils ont les mêmes degrés. Nous citons l'exemple de deux composantes de deux voisinages des sommets u et v de la figure 3.12, les matrices d'adjacence sont construites dans l'ordre décroissant des degrés, tel que les séquences de degrés pour les composantes $C_1(u)$ et $C_2(v)$ sont respectivement : $Seq(C_1(u)) = \{3,2,2,1\}$ et $Seq(C_2(v)) = \{2,2,2,2\}$. Pour rendre ces matrices identiques, nous devons ajouter 4 arêtes au total dans les deux composantes. Autrement dit, modifier chacune des deux matrices $M(C_1(u))$ et $M(C_2(v))$ (comme illustré en rouge). Modifier la matrice revient à exprimer l'ajout d'une arête et donc la valeur de la case correspondante au lien entre deux sommets devient 1.
Par contre si nous faisons la permutation entre les sommets 7 et 8 ayant les mêmes degrés dans la matrice de $C_2(v)$, nous obtenons une autre matrice d'adjacence $M'(C_2(v))$, et ainsi nous pouvons ajouter que 2 arêtes, une arête dans chacune des deux composantes (comme illustré en vert), ce qui revient à réduire le nombre d'arêtes ajoutées à 2 arêtes au lieu de 4.





	1	**2**	**3**	**4**
1	0	1	1	1
2	1	0	1	0_1
3	1	1	0	0_{11}
4	1	0_1	0_{11}	0

$M(C_1(u))$

	5	**6**	**7**	**8**
5	0	1	1	0_1
6	1	0	0_1	1
7	1	0_1	0	1
8	0_1	1	1	0

$M(C_2(v))$

	5	**6**	**8**	**7**
5	0	1	0_1	1
6	1	0	1	0
8	0_1	1	0	1
7	1	0	1	0

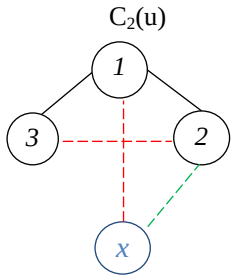
$M'(C_2(v))$

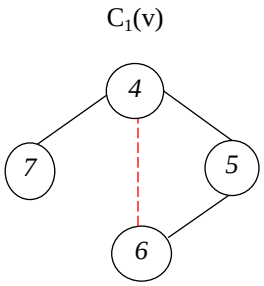
Figure 3.12 : Illustration d'anonymisation de deux composantes de voisinage avec le même nombre de sommets (les arêtes en pointillés représentent les arêtes ajoutées).

La similarité entre deux composantes avec un nombre différent de sommets est effectuée en vérifiant si les deux composantes sont sous-graphe isomorphes, c'est-à-dire, est ce que la grande composante contient un sous-graphe isomorphe à la petite composante, autrement dit on compare les matrices d'adjacence représentant les deux composantes comme suit : nous

cherchons si la grande matrice contient une sous matrice identique à la petite matrice, en effectuant toutes les combinaisons possibles des sommets de la grande matrice, en permutant juste les sommets ayant les mêmes degrés, et ceci dans le même but de réduire autant que possible le nombre d'arêtes ajoutées. Ensuite, pour rendre ces matrices identiques des sommets et des arêtes peuvent être ajoutés.

Dans l'exemple de la figure 3.13, nous avons les composantes $C_2(u)$ et $C_1(v)$ et leurs matrices d'adjacence correspondantes $M(C_2(u))$ et $M(C_1(v))$. Si nous comparons ces deux matrices telles qu'elles, pour les rendre identiques et que les composantes soient isomorphes, on doit ajouter un sommet x (soit un sommet existant ou un faux sommet selon les conditions qui seront expliquées dans la section 8.2.4) et 2 arêtes à la composante $C_2(u)$ ainsi qu'une arête à la composante $C_1(v)$ reliant les sommets 4 et 6 (comme illustré en rouge).
L'ajout d'un nouveau sommet dans la composante revient à modifier la matrice d'adjacence par l'insertion d'une nouvelle colonne et d'une nouvelle ligne.
Par ailleurs, si nous faisons une permutation entre les sommets 6 et 7 ayant les mêmes degrés, nous obtenons une nouvelle matrice d'adjacence $M'(C_1(v))$, nous remarquons que la matrice $M'(C_1(v))$ contient une sous matrice identique à $M(C_2(u))$, ce qui revient à ajouter juste un sommet x et une arête à la composante $C_2(u)$, et ceci produit un coût beaucoup moins élevé en comparant avec la matrice $M(C_1(v))$.





	1	2	3	x
1	0	1	1	1,0
2	1	0	0_1	0,1
3	1	0_1	0	0,0
x	1,0	0,1	0,0	0,0

$M(C_2(u))$

	4	5	6	7
4	0	1	0_1	1
5	1	0	1	0
6	0_1	1	0	0
7	1	0	0	0

$M(C_1(v))$

	4	5	7	6
4	0	1	1	0
5	1	0	0	1
7	1	0	0	0
6	0	1	0	0

$M'(C_1(v))$

Figure 3.13 : Illustration d'anonymisation de deux composantes de voisinage avec nombre de sommets différent (les arêtes en pointillés représentent les arêtes ajoutées).

8.2.4 Méthode d'ajout de nœuds

Rappelons que l'ajout de nœuds est sollicité lors de l'anonymisation de deux voisinages. Lors du traitement des graphes de voisinage $Neighbor_G(u)$ et $Neighbor_G(v)$ avec $|V(Neighbor_G(u))| > |V(Neighbor_G(v))|$ pour qu'ils soient identiques, de nouveaux nœuds doivent être introduits dans $Neighbor_G(v)$. Pour améliorer l'utilité du graphe publié, la stratégie d'ajout de « faux nœud» devrait être envisagée dans cette étape.
Soit $Neighbor_G(u)$ le voisinage du sommet u, $C_1(Neighbor_G(u))$ la composante de voisinage du sommet u nécessitant l'ajout de sommet. Ici, on choisit entre l'ajout de nœud existant et l'ajout d'un faux nœud dans le but de préserver autant que possible la distance moyenne entre

u et le reste des sommets du graphe. Autrement dit, la nouvelle distance moyenne doit être aussi proche que possible à la distance moyenne dans le graphe original.

L'algorithme 3 représente la méthode de sélection d'un nœud à ajouter à la composante $C_1(Neighbor_G(u))$. Notre algorithme sélectionne préférentiellement un nœud existant dans le graphe qui satisfait les conditions suivantes:

- Le nœud le plus proche au nœud u parmi les nœuds non anonymisés ou déjà anonymisés qui préserve la distance moyenne entre u et le reste des sommets du graphe.
- Le nœud avec le plus petit degré
- Le nœud avec label le plus proche

Si ces conditions ne sont pas satisfaites, un faux nœud doit être ajouté.

En outre, les nœuds qui sont déjà dans Neighbor(u) ne peuvent pas être reliés à u, comme ils sont déjà reliés à u.

La sélection du nœud approprié se déroule selon les étapes suivantes :

1. D'abord, les distances entre le sommet u et le reste des sommets du graphe G sont calculées en utilisant l'algorithme de Dijkstra [7]. Ensuite, nous calculons la moyenne de ces distances soit cette moyenne «dist_moy_originale».

Considérons l'exemple déjà illustré dans la figure 3.2(b) pour montrer un cas d'anonymisation qui utilise l'algorithme 3. Dans cet exemple, supposons que nous voulons anonymiser les voisinages de deux sommets 2 et 6 : nous avons besoin d'ajouter un sommet au voisinage du sommet u=6 pour qu'il soit isomorphe au voisinage du sommet 2. La moyenne originale entre le sommet 6 et le reste des sommets du graphe dist_moy_originale = 2,9.

2. Nous considérons d'abord les sommets de V(G) qui sont non anonymisés (marqués « unanonymized »). Nous calculons les distances entre le sommet u et ces sommets. Puis, trouvons parmi ces sommets un sommet *w* le plus proche de u (c.-à-d. ayant la plus petite distance avec u). S'il y a plus d'un candidat ayant la même plus petite distance, nous choisissons celui ayant le plus petit degré. S'il y a plus d'un sommet satisfaisant ces deux conditions (càd il existe plus d'un sommet ayant la même plus petite distance avec u avec le même degré), nous l'ajoutons à l'ensemble des nœuds candidats Q.

3. L'ajout d'une arête entre le sommet u et un sommet w modifiera la valeur de la distance à 1 car ils seront directement connectés. Ayant cette connaissance, si l'ensemble candidat Q n'est pas vide, pour chaque sommet w appartenant à cet ensemble, nous recalculons la moyenne des distances entre u et le reste des sommets du graphe en ajoutant w, notons cette moyenne «dist_moy_ajout_sommet_non-anonymisé». Les distances calculées reflètent la distance après que l'arête ait été ajoutée entre le sommet u et un sommet *w* sans l'ajouter réellement. Nous choisissons le sommet w qui produit la moyenne «dist_moy_ajout_sommet_non-anonymisé» la plus proche de «dist_moy_originale». Si on a plusieurs sommets appartenant à Q satisfaisant cette condition, nous choisissons celui ayant le label le plus proche en termes de pénalité normalisée de la certitude. Notre but ici est de maintenir autant que possible la distance moyenne entre u et le reste des sommets du graphe.

Dans notre exemple illustré dans la figure 3.14, le sommet le plus proche au sommet 6 est le sommet non anonymisé *w* = 0, car il satisfait les conditions requises. Une arête sera ajoutée entre 6 et 0 comme illustré en rouge, et la distance entre 6 et 0 est changée de 3 à 1 et la

moyenne entre le sommet 6 et le reste des sommets deviendra dist_moy_ajout_sommet_non-anonymisé=2,6.

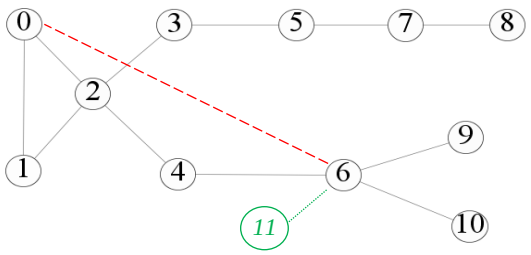


Figure 3.14 : Illustration d'ajout de sommet existant ou de faux sommet

4. D'autre part, nous calculons la moyenne des distances entre u et les autres sommets en simulant l'ajout d'un faux sommet *w'* sans l'ajouter réellement, soit « dist_moy_ajout_faux_sommet ». Dans notre exemple, si nous ajoutons un faux sommet *w'* =11 (illustré en vert) la moyenne des distances entre le sommet 6 et le reste des sommets est devenue dist_moy_ajout_faux_sommet =2,73.

5. A ce stade, nous comparons « dist_moy_ajout_sommet_non-anonymisé » et « dist_moy_ajout_faux_sommet » avec « dist_moy_originale ».

- Si la valeur « dist_moy_ajout_sommet_non-anonymisé » est plus proche de « dist_moy_originale » alors notre choix se porte sur *l'ajout du sommet existant non anonymisé*.
- Dans le cas contraire, nous essayons de trouver parmi les sommets déjà anonymisés un sommet w satisfaisant la condition de distance moyenne. Nous procédons de la même manière que pour les sommets non anonymisés pour obtenir l'ensemble des nœuds candidats Q' et choisir w. Nous calculons «dist_moy_ajout_sommet_déjà-anonymisé » la moyenne des distances entre u et le reste des sommets en ajoutant le sommet déjà anonymisé w.
    - Si «dist_moy_ajout_sommet_déjà-anonymisé » est plus proche de « dist_moy_originale » alors on *ajoute un nœud existant déjà anonymisé* à la composante $C_1(Neighbor_G(u))$, nous marquons *w* et ses *(k -1)* autres sommets anonymisés dans le même groupe comme «unanonymized », ainsi nous les réinsérons dans la liste « vertexList ».
    - Sinon, l'algorithme *génère un faux nœud* w' et l'ajoute à $C_1(Neighbor_G(u))$, ainsi que à la liste « vertexList » pour l'anonymiser dans les prochaines itérations du processus d'anonymisation.

Notons qu'en priorité nous choisissons d'ajouter un sommet existant satisfaisant la condition de distance moyenne (sommets non anonymisé puis sommets déjà anonymisé) dans le but de réduire autant que possible le nombre de faux sommets ajoutés. Dans le cas où il n'existe pas de nœuds non anonymisés à ajouter, le choix se portera sur le choix entre l'ajout de sommets déjà anonymisés ou l'ajout de faux sommets selon les conditions décrites précédemment.

Dans l'exemple, « dist_moy_ajout_faux_sommet» est plus proche de « dist_moy_originale », et nous n'avons pas des sommets déjà anonymisé pour choisir entre eux. Par conséquent, le meilleur cas pour préserver la distance moyenne est d'ajouter réellement un faux sommet au voisinage du sommet 6 (comme illustré en vert). Ainsi, nous concluons que la distance entre les nœuds est mieux préservée en ajoutant un faux sommet.

Finalement, l'algorithme généralise les labels si nécessaire, et attribue aux faux nœuds des labels, de sorte que tous les groupes de sommets satisfont encore la condition du « k-anonymat ». En d'autres termes, le faux nœud, créé pendant le processus d'appariement entre deux composantes de voisinage, aura les mêmes labels que ceux du sommet d'origine avec qui on l'a fait correspondre. Dans notre exemple, le faux nœud 11 aura les labels: « Pédiatre » et « Grippe », qui sont les labels correspondants au nœud 3.

Algorithme 3 : Algorithme d'ajout de sommets

Entrée: C($Neighbor_G$(u)) : la composante de voisinage d'un sommet u nécessitant l'ajout de sommet
Sortie: un sommet existant ou un faux sommet à ajouter;

Début

Pour chaque sommet $v \in V(G)$ ***faire***
Calculer $d(u,v)$ // la distance entre u et v en utilisant l'algoithme de Dijkstra
Fin Pour
dist_moy_originale ← La moyenne des distances entre u et tous les sommets $v \in V(G)$

Pour chaque sommet « *v non anonymisé* » $\in V(G)$ ***faire***
D ← $d(u,v)$ // Ensemble contenant la distance entre u et tous les autres sommets v *non anonymisé*
Fin Pour
MinD ← le Min des distances dans D *

Pour chaque sommet « *v non anonymisé* » $\in V(G)$ tel que $d(u,v)$ =MinD ***faire***
Q←v tel que degré(v) est minimal; // Q : l'ensemble candidat des sommets non anonymisés qu'on peut ajouter
Fin Pour

Si Q ≠ ∅ **alors** // veut dire qu'il existe au moins un sommet non anonymisé à ajouter

Pour chaque sommet w ∈ Q **faire** // Créer l'ensemble contenant toutes les moyennes en ajoutant w
Moy← La moyenne des distances entre u et tous les sommets $v \in V(G)$ en ajoutant w
Fin Pour

dist_moy_ajout_sommet_non-anonymisé←élément de Moy tel que (|dist_moy_originale-Moy| est minimale et w produisant cette moyenne ayant le NCP minimal

dist_moy_ajout_faux_sommet← La moyenne des distances entre u et tous les sommets $v \in V(G)$ en ajoutant un faux sommet w'

Si (|dist_moy_originale-dist_moy_ajout_sommet_non-anonymisé|< |dist_moy_originale- dist_moy_ajout_faux_sommet|)
alors
Retourner w // dist_moy_ajout_sommet_non-anonymisé est plus proche de dist_moy_originale
Sinon
// Nous essayons de trouver un sommet déjà anonynisé de la même manière que * pour avoir Q' et dist_moy_ajout_sommet_déjà-anonymisé

Si (|dist_moy_originale - dist_moy_ajout_sommet_déjà-anonymisé|
< |dist_moy_originale - dist_moy_ajout_faux_sommet |) **alors**
w←le sommet déjà anonymisé le plus proche de u satisfaisant la condition de distance et degré et label
Marquer w et les sommets dans son groupe comme « unanonymized »
Réinsérer w et les sommets appartenant à son groupe dans *Vertexlist*
Retourner w **
Sinon
Générer un faux sommet w'
vertexList←w' // pour l'anonymiser
Retourner w' // dist_moy_ajout_faux_sommet est plus proche de dist_moy_originale
Fin si

Fin Si

Sinon // Si nous ne pouvons trouver aucun sommet non anonymisé à ajouter
Trouver un sommet déjà anonymisé de la même manière que **
Fin Si

Fin

En utilisant le graphe social présenté sur la figure 3.2 nous illustrons sur la table 2, les valeurs de quelques propriétés structurelles du graphe anonymisé en utilisant les deux méthodes d'anonymisation : méthode d'ajout d'arêtes de Zhou et Pei et notre méthode proposée:

	Graphe original	Zhou et Pei	Méthode proposée
Diamètre	7	4	7
Rayon	4	3	4
APL	3.109090909090909	2.4727272727272727	3.1818181818181817
Densité	0,200	0,236	0,197

Table 2: Propriétés structurelles en ajoutant des liens VS en ajoutant de faux sommets

Nous remarquons que les valeurs des propriétés structurelles du graphe anonymisé avec la méthode proposée d'ajout de faux nœuds sont plus proches des valeurs des propriétés du graphe original en comparant avec celles de la méthode d'ajout de liens, et ainsi elles sont mieux préservées.

9 Conclusion

Plusieurs travaux ont été réalisés au sujet de l'anonymisation des graphes sociaux contre l'attaque de voisinage, qui ont pour but de protéger l'identité des utilisateurs contre un attaquant ayant comme connaissance de base « les voisinages » de certains individus cibles.

Parmi les solutions existantes, celle proposée par Zhou et Pei [54] et améliorée par Tripathy et al [64] qui sont présentées dans le chapitre 2. Elles demeurent des solutions garantissant la préservation de l'anonymat des individus présents dans le graphe anonymisé mais qui ont des limites concernant l'utilité, notamment la préservation de l'APL du graphe anonymisé résultant. Ce qui nous a conduit à proposer une nouvelle approche d'anonymisation basée sur l'ajout de faux nœuds en plus de l'ajout de liens.

Dans le prochain chapitre, nous décrirons la mise en œuvre de l'approche ainsi que les résultats des tests effectués pour démontrer l'apport dans la préservation de l'APL et analyser l'impact sur d'autres propriétés structurelles tels que : le diamètre du réseau, le rayon, les distances entre les différents sommets, etc…, qui ont tous un effet direct sur l'utilité des résultats d'anonymisation.

1 Introduction

Après avoir décrit les fondements théoriques, nous abordons dans ce chapitre l'aspect implémentation afin de mettre en œuvre notre algorithme d'anonymisation baptisé « AnonSN ». L'objectif étant d'évaluer notre approche d'amélioration de l'utilité du graphe anonymisé résultant.

Nous évaluons notre algorithme proposé en comparant les résultats de l'algorithme de référence déjà proposé par Zhou et Pei [54] que nous avons aussi implémenté, avec les observations expérimentales de notre nouvel algorithme sur l'ensemble de données de réseaux sociaux synthétiques ainsi que sur l'ensemble des données réelles. Plus précisément, nous observons comment l'APL est préservée par notre nouvel algorithme d'anonymisation, et nous analysons l'impact sur d'autres propriétés structurelles tels que : le diamètre, le rayon, la densité, etc….

Nous présentons et nous justifions tout d'abord les outils utilisés, ensuite les étapes de l'implémentation et cela en commentant les résultats des modules implémentés en utilisant à la fois les données synthétiques et réelles. Enfin, nous allons exposer et commenter les différents tests effectués.

2 Les outils utilisés

Pour la réalisation de notre « application », nous avons opté pour les outils de développement suivants :

- Windows 7 comme système d'exploitation
- Langage JAVA (JDK 1.6) comme langage de programmation
- NetBeans 7.2.1 comme environnement de développement
- Gephi comme outil de représentation et d'analyse de réseaux sociaux
- Pajek comme outil de génération de données synthétiques

2.1 Le langage de programmation « JAVA »

Afin d'implémenter notre algorithme, nous avons opté pour le langage Java comme outil de développement. Ce choix est dû, d'une part, au fait que ce langage est indépendant de toute plateforme et qu'il est orienté objet. Parmi les avantages du langage Java, on trouve notamment que c'est un langage : [103]

- **Orienté Objet :** Java est un langage full object c'est-à-dire qu'il respecte une approche orienté objet de la programmation, sans qu'il soit possible de programmer autrement. En clair contrairement à d'autres langages comme C++ on ne peut faire que de la programmation orienté objet avec Java.

- **Portable :** Un programme écrit en Java peut être exécuté sans aucune modification sur un autre système, à condition bien sûr qu'un environnement d'exécution (i.e. machine virtuelle) soit disponible sur ce dernier.

- **Interprété :** Un programme écrit en Java est exécuté par un interpréteur, qui traduit en temps réel les instructions Java en instructions exécutables par le système hôte. Une source écrit en Java n'est pas exécutée telle quelle. En fait, on transforme une source Java

en un fichier qui sera interprété par une machine virtuelle. Il convient de noter que la portabilité de Java découle du fait qu'il soit interprété.

- **Sécurisé :** La sécurité et la sureté d'exécution des programmes font partie des points forts du langage Java. Elles consistent à assurer que les classes utilisées dans un programme n'effectuent pas d'opération mettant en péril l'exécution du programme, l'intégrité du système ou la confidentialité des données.

Java est donc un langage puissant et performant, tirant expérience des autres langages apparus avant lui. Ces caractéristiques nous ont poussées à l'utiliser comme langage de programmation pour implémenter l'algorithme de Zhou et Pei ainsi que notre algorithme « AnonSN ».

2.2 Outils de représentation et d'analyse «Gephi »

Gephi est un logiciel open source, créé en 2008 par une équipe de 4 ingénieurs en informatique. Il permet la visualisation, l'analyse et l'exploration en temps réel des graphes. Doté d'une architecture flexible et multitâche, apporte de nouvelles possibilités de travailler avec des ensembles de données complexes et produire des résultats visuels précieux. Il offre un accès facile et large aux données du réseau et permet la spatialisation, le filtrage, la navigation, la manipulation et le clustering. Gephi offre le calcul des métriques les plus courantes comme l'intermédiarité, la proximité, le diamètre, le coefficient de clustering, l'APL, PageRank, la détection de communautés en utilisant la modularité et les générateurs aléatoires, etc [36].
Les travaux produits dans Gephi sont exportables dans plusieurs formats, notamment le PDF. Les formats supportés par Gephi sont: GEXF14, GDF, DOT, GraphML. Il peut également exporter les données importées aux plusieurs formats notamment csv, qu'on a adopté pour représenter les graphes utilisés dans nos tests. La figure 4.1 représente un aperçu de l'interface de Gephi. Cette interface se structure autour de 3 onglets pour répondre à ces différents besoins : [88]

- **Une vue d'ensemble** pour analyser l'information

- **Un laboratoire des données** pour voir nos données : se présentant sous la forme d'un simple tableau, nous pourrons manipuler nos informations comme nous l'aurions fait sous Excel. Une particularité, le laboratoire de données possède deux onglets en haut à gauche, un onglet Nœuds, et un onglet lien. nous pourrons donc passer des données concernant les acteurs de notre réseau (les comptes Twitter par exemple), aux données reliant ses acteurs (qui suit /mentionne qui).

- **La zone de classement et de partition :** dans cette zone, nous pouvons colorier les données en fonction des paramètres obtenus par l'analyse statistique, ou séparer nos données pour leur appliquer des couleurs différentes. Nous pourrons par exemple séparer deux groupes sur le schéma pour les classer en fonction de différentes informations.

- **La zone de spatialisation** : cet onglet nous permet de choisir un algorithme pour replacer les nœuds (par exemple comptes Twitter), au mieux et nous permettre de visualiser leurs interactions.

- **Un onglet de filtres et de statistiques** : avec cet outil, nous pouvons retirer certains nœuds (comptes Twitter) de notre réseau, filtrer l'information en fonction de certains paramètres, mais aussi effectuer des analyses statistiques en calculant les différentes propriétés du graphe.

- **L'affichage des données :** Cet onglet permet de faire varier la taille des nœuds, des liens entre les nœuds, et d'afficher les noms des nœuds.

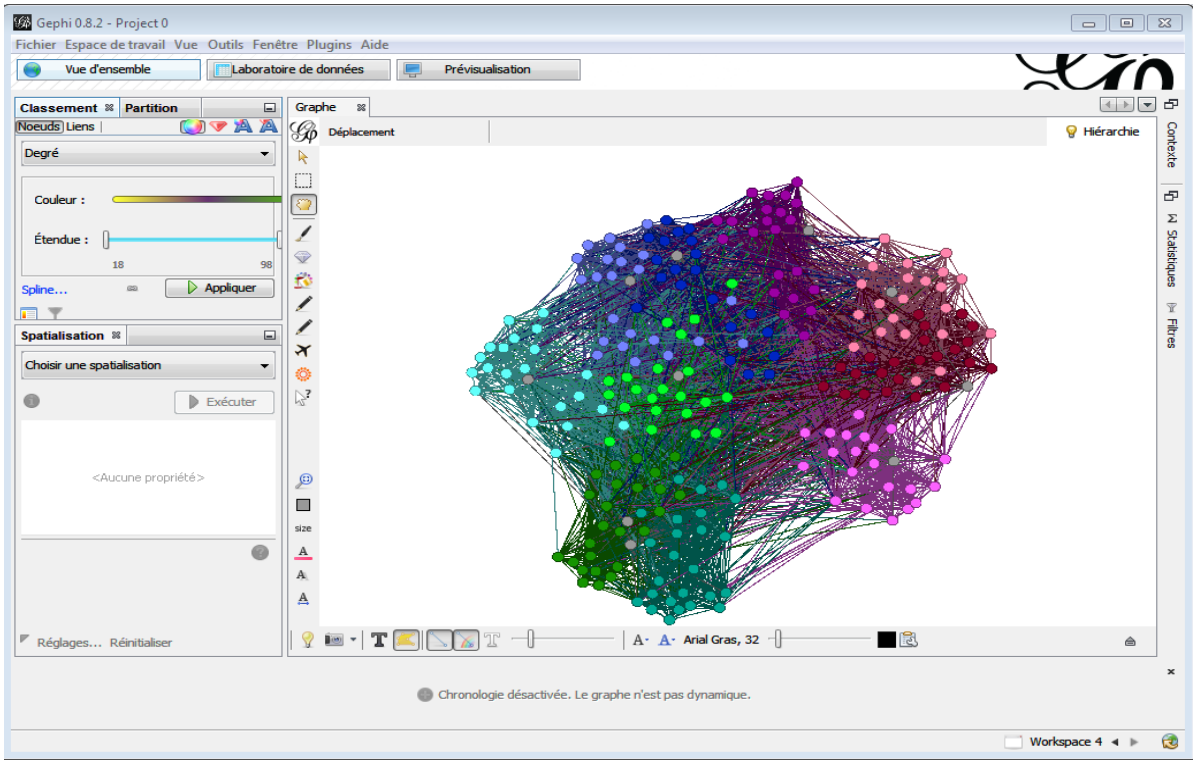


Figure 4.1 : Aperçu de l'interface de Gephi

Nous citons quelques raisons pour lesquelles nous avons choisi d'utiliser Gephi :

- Outil libre et gratuit
- Interface de Gephi disponible en français, espagnol, japonais, anglais, russe, et autres.
- Près de 1600 publications universitaires citent Gephi.
- Son forum est toujours actif (https://forum.gephi.org/)
- C'est un logiciel écrit en Java pour Mac, Windows et Linux
- Il permet une visualisation attractive des données.
- Un écosystème de plugins et d'applications apparentées.
- Il possède plusieurs algorithmes de calcul.
- Utilise des données importées de bases de données spécifiques (Pilotes : MySQL, SQL Server, PostgreSQL, SQLite, Teradata).
- Il permet d'exporter des données sous divers formats (.pdf, .png, .csv, .gdf, .net,..etc).

2.3 Outil de génération de données synthétiques « Pajek »

« Pajek » est un logiciel d'analyse et de visualisation de réseaux. Développé par deux chercheurs slovènes, Vladimir Batagelj et Andrej Mrvar, il a le grand mérite d'être gratuit et puissant, ce qui lui a permis de s'imposer comme un des outils les plus utilisés en analyse des réseaux [17]. Il peut générer des graphes sans échelle avec caractéristique de petit monde, qui sont les deux propriétés les plus importantes pour les réseaux sociaux.

« Pajek » présente plusieurs avantages : il est gratuit, il fonctionne aussi bien sous Windows, Mac OS ou Linux, il permet d'étudier des graphes de grande taille (comportant plusieurs milliers de « nœuds »), et il est compatible avec les autres logiciels existants (notamment *Ucinet* et *R*). En outre, son site internet (http://pajek.imfm.si) propose une documentation fournie, et de nombreux jeux de données disponibles pour démonstration [17]. La figure ci-dessous présente l'interface du logiciel :

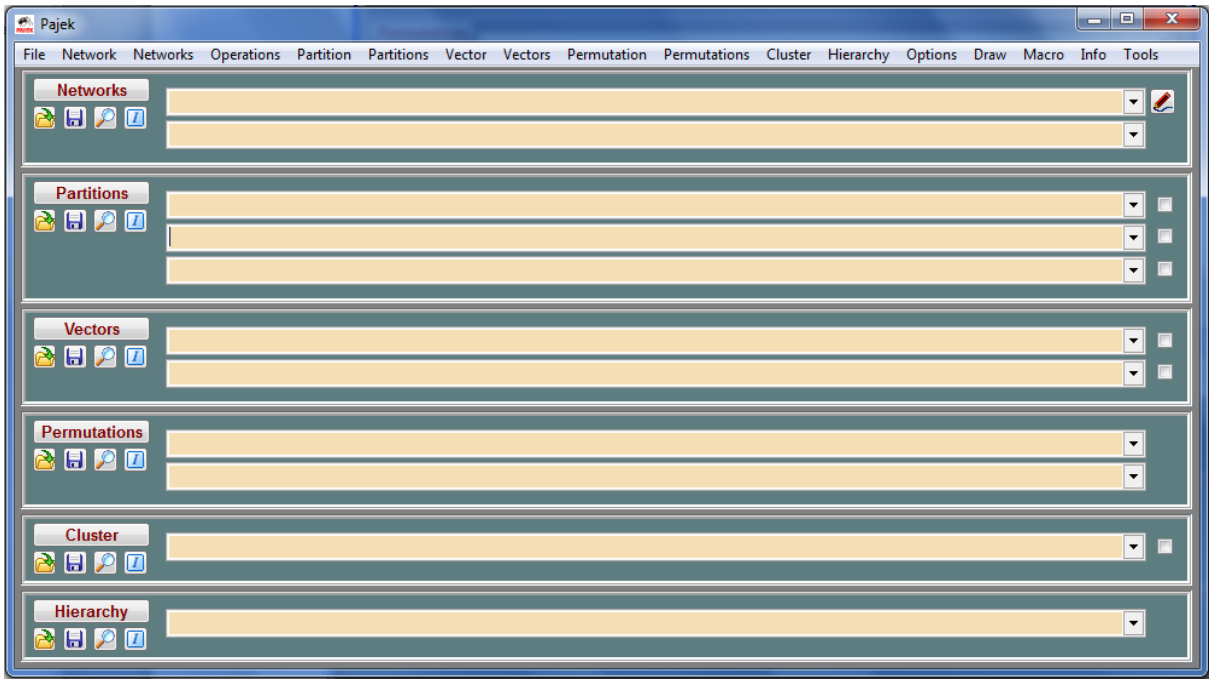


Figure 4.2 : Interface du logiciel « Pajek »

Dans notre cas, nous avons installé la dernière version du logiciel « version 4.08 » pour Windows 32 bits [45].

3 La représentation d'un graphe en mémoire

Il existe plusieurs manières de représenter un graphe en mémoire. Une première solution est de l'encoder à l'aide d'une matrice d'adjacence M de taille n x n dans laquelle :

$$M_{i,j} = \begin{cases} 1 \text{ si } (i,j) \in E \\ 0 \quad \text{sinon} \end{cases}$$

Ce codage permet de vérifier l'existence d'un lien en temps constant, mais une requête d'adjacence, qui consiste à lister les voisins d'un sommet *v* demande de parcourir une ligne entière, et s'effectue en O(n), et le chargement de la matrice en mémoire demande $\Theta(n^2)$, ce qui est inefficace lorsque le graphe est dense. Dans ce cas, un autre codage consiste à utiliser

une représentation en liste d'adjacence, dans laquelle on stocke pour chaque sommet la liste de ses voisins. Cette représentation permet de réduire l'espace nécessaire au chargement en mémoire à Θ (m), et le parcours d'un voisinage se fait en temps optimal : Θ (d(u)). Cependant, cette structure est moins efficace que la matrice d'adjacence pour tester l'existence d'un lien : Θ(d(u)), que nous avons besoin d'effectuer fréquemment dans notre application, d'où on a utilisé les matrices d'adjacence dans l'implémentation de notre outil, tel que toutes les structures utilisées (graphe, voisinage, composantes de voisinage) sont représentées à l'aide des matrices d'adjacences [12].

4 Interfaces de l'outil développé « AnonSN »

Nous présentons ici l'outil d'anonymisation « AnonSN » que nous avons mis en œuvre dans le cadre de notre projet, l'objectif est de fournir un guide complet permettant aux utilisateurs de pouvoir utiliser notre outil dont l'interface principale est illustrée sur la figure 4.3 ci-dessous :

Figure 4.3 : Interface principale

Le processus d'anonymisation se déroule selon les étapes suivantes :

La première étape consiste à choisir un fichier en entrée contenant la matrice d'adjacence représentant le graphe social à anonymiser comme démontré dans la figure 4.4. Le fichier d'entrée doit être en format « csv », d'où on a exporté tous nos données de graphes sociaux réels et synthétiques vers ce format en utilisant le logiciel « Gephi ».

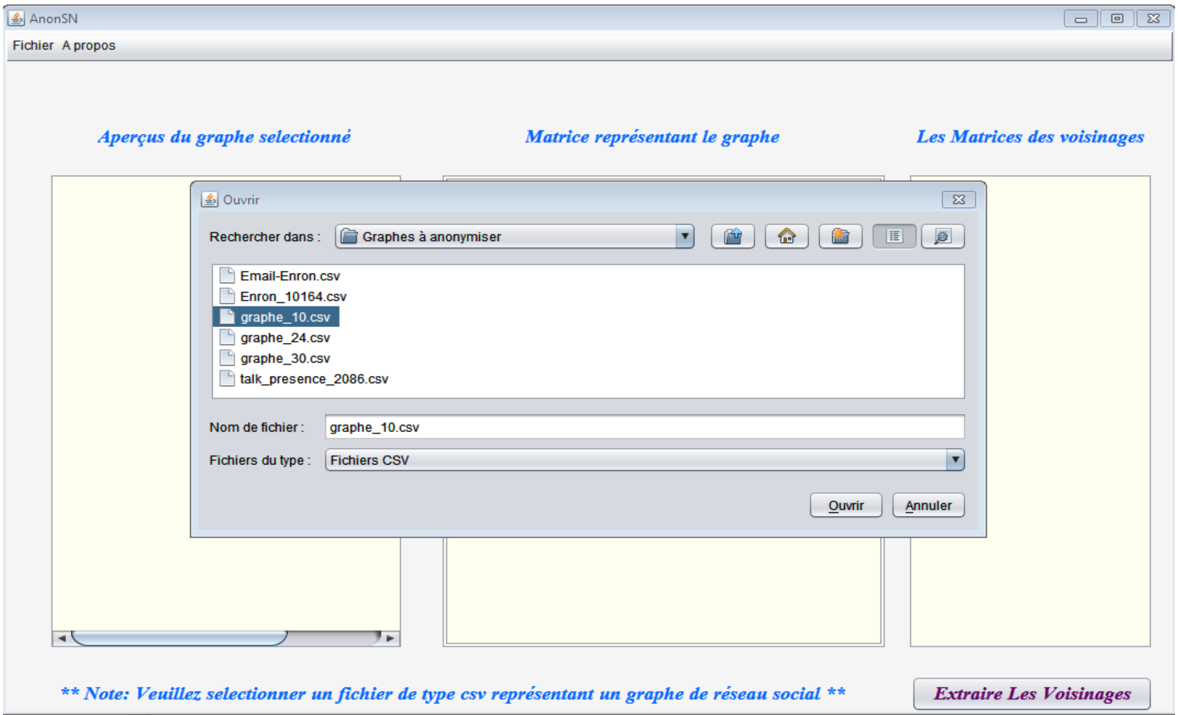
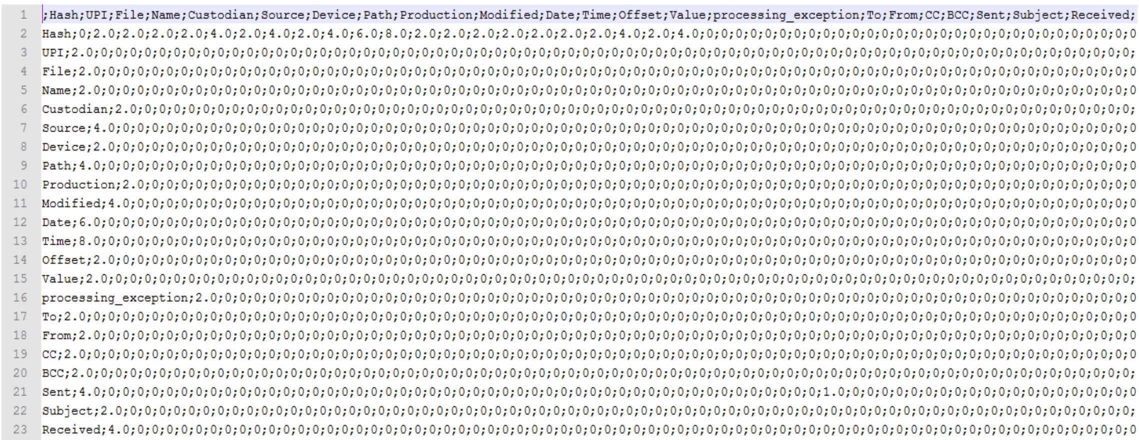


Figure 4.4 : Sélection d'un fichier en format CSV



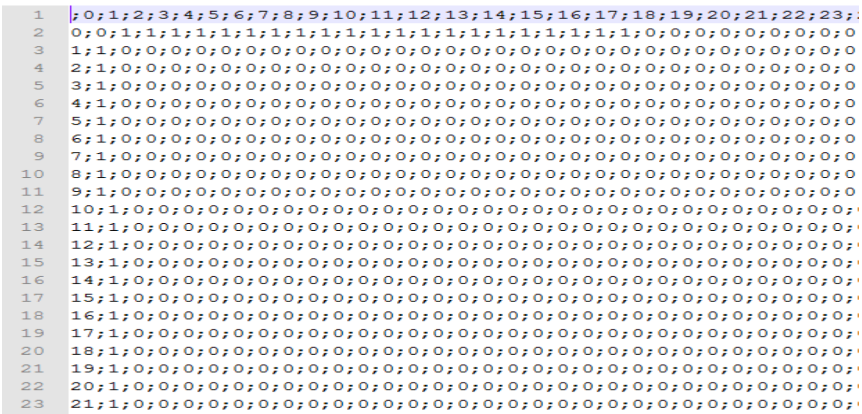


Figure 4.5 : un graphe présenté en format csv et son anonymisation naïve

Après que le fichier contenant le graphe est sélectionné, nous effectuons une anonymisation naïve de ce graphe social, en remplaçant tous les identifiants des différents nœuds par des identifiants aléatoires comme illustré dans la figure 4.5, et ainsi nous construisons un fichier .csv représentant le graphe social naïvement anonymisé.

Une fois le fichier représentant le graphe social naïvement anonymisé est construit, les voisinages des différents sommets constituant le graphe sont extraits, la matrice d'adjacence du graphe ainsi que les matrices d'adjacence des différents voisinages et un aperçu de ce graphe sont créés et affichés comme illustré dans la figure 4.6.

Une fois affiché, en cliquant sur « Anonymiser le graphe », une autre interface apparaît sur laquelle l'utilisateur est invité à introduire quatre paramètres très importants pour l'anonymisation : le paramètre d'anonymisation k, et trois paramètres α, β, et γ qui servent à calculer le coût d'anonymisation (voir figure 4.7). Ensuite, la procédure d'anonymisation pourra commencer.

Après avoir terminé l'exécution de la procédure d'anonymisation telle que déjà expliquée dans le chapitre 3 en ajoutant des arêtes et des sommets existants ou des faux sommets, la sortie de l'algorithme est un graphe anonymisé satisfaisant la condition de k-anonymat. Ainsi, pour chaque sommet il y'a au moins (k-1) autres sommets ayant des voisinages isomorphes. Le graphe résultant peut être enregistré dans un fichier sous le même format « csv » comme démontré dans la figure 4.8.

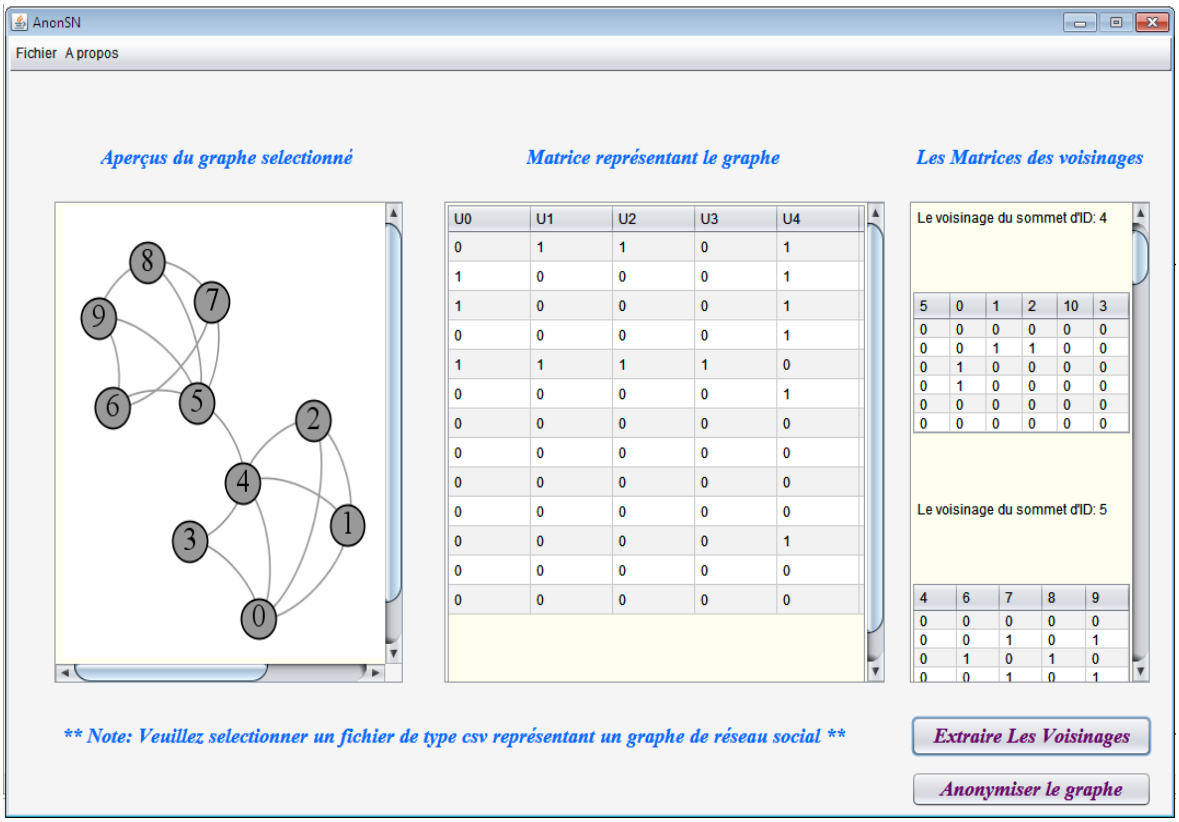


Figure 4.6 : Aperçu de la matrice d'adjacence représentant le graphe ainsi que les matrices de voisinage

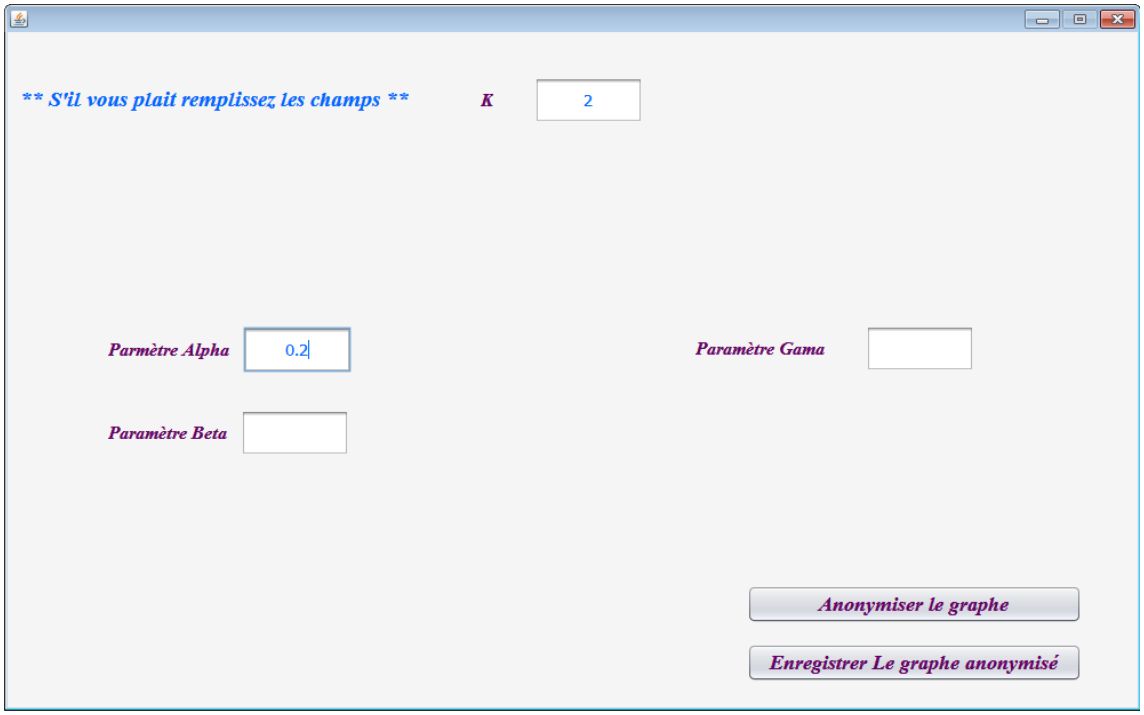


Figure 4.7 : Remplissage des paramètres d'entrée

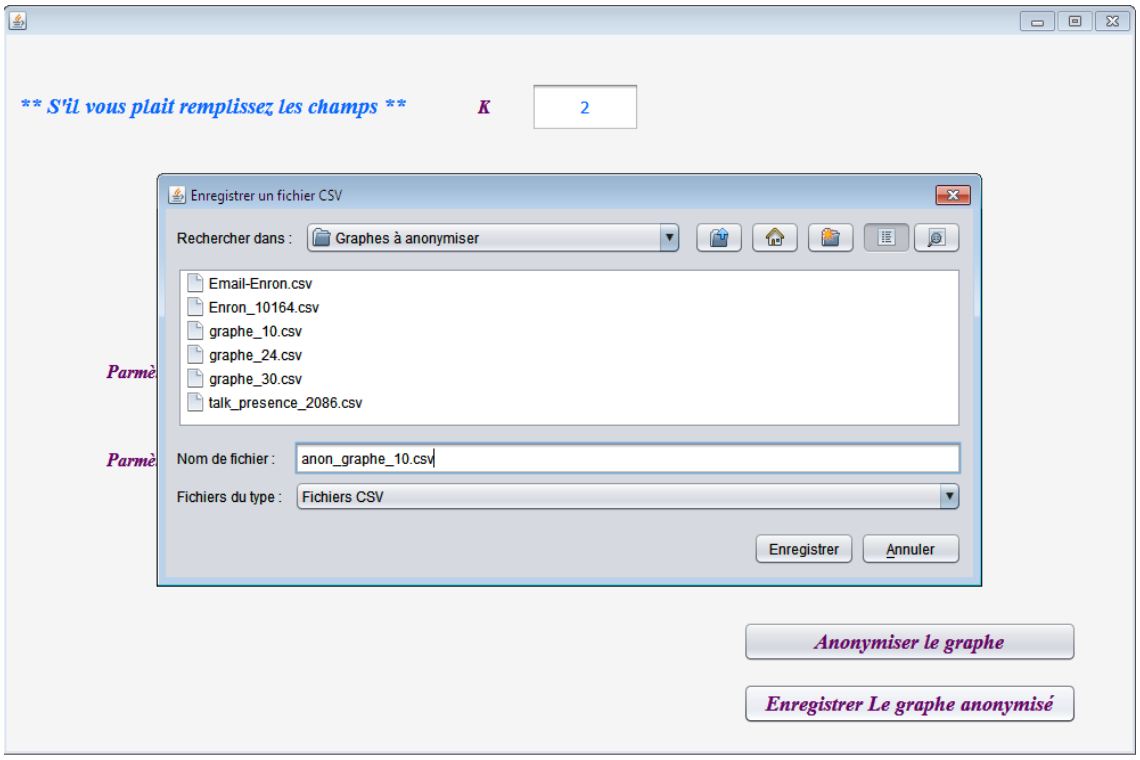


Figure 4.8 : Enregistrer le graphe anonymisé

5 Expérimentation

Dans cette section, nous décrivons les différentes expériences effectuées sur des ensembles de données réelles et synthétiques. Ainsi, nous discutons les résultats pour évaluer et illustrer les performances de notre approche proposée en comparant notre approche à l'approche existante de Zhou et Pei [54].

Nous commençons d'abord par décrire le besoin d'implémenter le modèle de référence de Zhou et Pei. Ensuite, nous décrivons notre environnement expérimental et le jeu de données utilisé pour nos tests, ainsi que les mesures d'évaluation de notre approche. Enfin, nous présentons nos résultats et discussions.

5.1 Le modèle de référence de Zhou et Pei

Selon l'énoncé du problème défini dans le chapitre 3, nous avons besoin d'implémenter le modèle de Zhou et Pei « k-voisinage » [54] utilisant l'ajout d'arêtes et les matrices d'adjacences pour les tests d'isomorphismes proposé par Thripathy et al [64]. Nous avons implémenté ce modèle pour qu'il sera testé et comparé avec notre modèle en utilisant la même configuration (paramètre d'anonymat k, paramètres de calcul de coût d'anonymisation, …etc.), et cela pour pouvoir tester et prouver les performances de notre approche proposée.

5.2 Environnement expérimental

Toutes les expériences que nous avons effectué ont été mises en œuvre sur une machine 32 bits avec Windows 7, un processeur Intel Core 2 duo 2.50GHz, et 4 Go de RAM. Pour les grands graphes, nous avons effectué les tests sur le Cluster Ibnbadis disponible au niveau du centre de calcul du CERIST. Nous avons exécuté notre code sur la version 1.8.0_77 de JRE 32 bits. De plus, nous avons utilisé les paramètres de la fonction de coût d'anonymisation comme suit : $\alpha = 0.0$, parce que notre objectif est la structure de graphe et non pas les labels. $\beta = \gamma = \delta = 1$, car nous avons donné la même chance ou le même poids pour l'ajout d'arêtes, sommets existants, et faux sommets. Notons que nous avons utilisé ces paramètres dans toutes nos expériences.

5.3 Le jeu de données utilisé

Nous étudions les propriétés structurelles illustrées dans le chapitre 3 sur les versions originales et anonymisées des ensembles de données synthétiques et réelles. Le premier ensemble de données est une famille de graphes synthétiques générés à l'aide du logiciel « Pajek », le deuxième ensemble de données représente des graphes réels. Nous détaillons ci-dessous chacun des deux ensembles utilisés dans nos expériences :

5.3.1 Ensemble de données synthétiques

Nous avons généré deux graphes synthétiques en utilisant le logiciel « Pajek » avec les deux propriétés les plus importantes des réseaux sociaux : petit monde et sans échelle qui modélise les réseaux sociaux du monde réel qui suivent une distribution de degrés en loi de puissance [21]. Ces graphes ont les paramètres suivants :

- **Graphe_40 :** avec le nombre de nœuds = 40, nombre d'arêtes = 51.
- **Graphe_345** : avec le nombre de nœuds = 345, nombre d'arêtes = 355.

5.3.2 Ensemble de données réelles

Pour pouvoir tester l'efficacité et la performance de notre algorithme, plusieurs sources fournissant des données de graphes sociaux réels peuvent être utilisées. Notre objectif ici est de définir quelques graphes sociaux qui ont reçu beaucoup d'attention dans la recherche et qui seront utiles pour nous dans toutes nos expérimentations, Ce sont des graphes accessibles au public sur internet.

- **Graphe d'Enron :** nous avons pris l'ensemble de communications par emails dans l'entreprise « Enron » disponible en ligne[21]. Ces données ont été initialement rendu publiques par la « Federal Energy Regulatory Commission » durant son enquête sur l'entreprise. Un nœud dans ce graphe représente une adresse e-mail. Une arête existe entre deux nœuds si au moins un message électronique a été envoyé d'un nœud à l'autre. C'est un ensemble de données représentatif utilisé dans l'analyse des réseaux sociaux et la recherche dans le domaine de l'anonymisation comme dans [48] et [53]. EDRM (Electronic Discovery Reference Model) fourni ces données sous format csv[22], qui représentent les résultats des tests du logiciel FreeEed avec les données d'Enron. Dans nos expérimentations, nous avons choisi trois graphes avec les paramètres suivants :
  - **Enron_1583 :** 1583 nœuds et 4212 arêtes.
  - **Enron_2579 :** 2579 nœuds et 6783 arêtes.
  - **Enron_3200 :** c'est un graphe qui était à 3231 nœuds, dans lequel on a pris la plus grande composante connexe contenant 3200 nœuds et 6267 arêtes.

- **Krackfr_CSV** : c'est un graphe social de 271 nœuds et 359 arêtes, disponible en format csv[23]. Ce sont des données de structure sociale cognitive collecté par David Krackhardt [102] auprès de 21 personnels de gestion dans une high-tech, entreprise de fabrication de machine pour évaluer les effets d'un programme récent d'intervention de gestion.

- **The UCI Network Data Repository [24] :** est un portail qui regroupe une collection de données de graphes issus de réseaux sociaux en ligne, réseaux de communication, collaboration entre auteurs, ...etc., pour faciliter l'étude scientifique des réseaux, Parmi les données disponibles nous avons choisis deux graphes de « **AMD Hope RFID Data »,** où les participants reçoivent des badges RFID qui les identifient de façon unique et les suivent à travers l'espace de conférence. L'ensemble de données détaille des descriptions de leurs intérêts, interactions via des messages instantanés, et leur emplacement au cours de la conférence. Les deux graphes que nous avons choisis ont les caractéristiques suivantes :
  - **Interest** : 434 nœuds et 1924 arêtes[25].
  - **Talk_presence** : 2086 nœuds et 35605 arêtes[26].

[21] https://www.cs.cmu.edu/~./enron/
[22] http://freeeed.org/index.php/documentation/testing-with-enron-data
[23] http://www.casos.cs.cmu.edu/computational_tools/data2.php
[24] https://networkdata.ics.uci.edu/index.php
[25] networkdata.ics.uci.edu/data/amdhope/hopeamd-export/interests.csv
[26] networkdata.ics.uci.edu/data/amdhope/hopeamd-export/talk_presence.csv

5.4 Exemple d'anonymisation

Considérons le graphe synthétique de 40 nœuds, les figures ci-dessous illustrent les résultats de son anonymisation selon les deux algorithmes de « Zhou et Pei » et « AnonSN » :

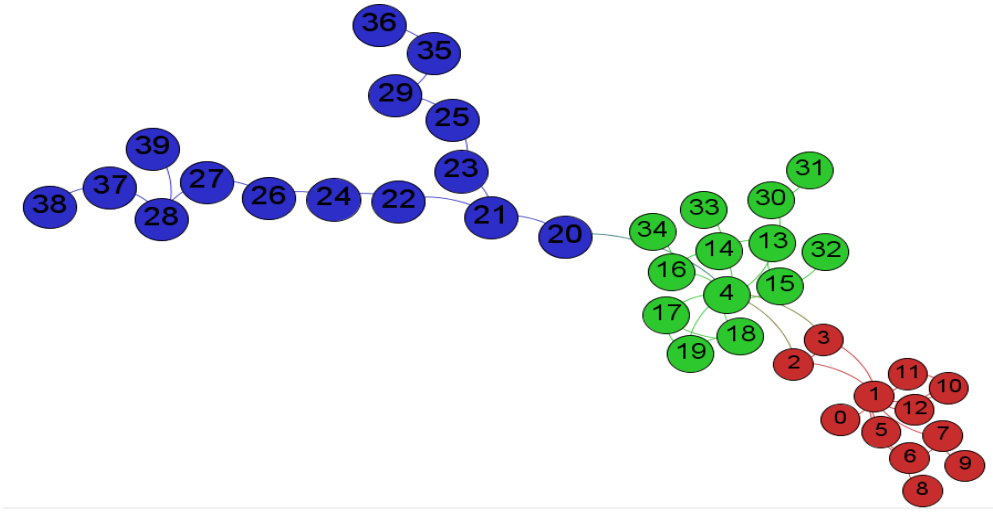


Figure 4.9 : Le graphe original

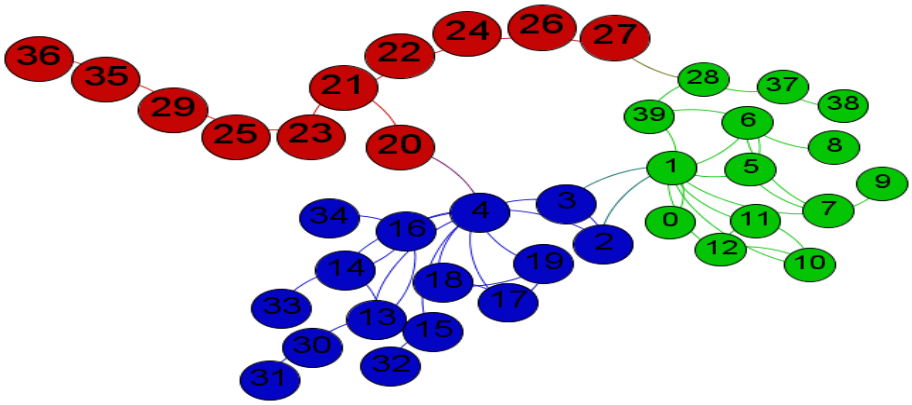


Figure 4.10 : Le graphe anonymisé à l'aide de l'algorithme de Zhou & Pei

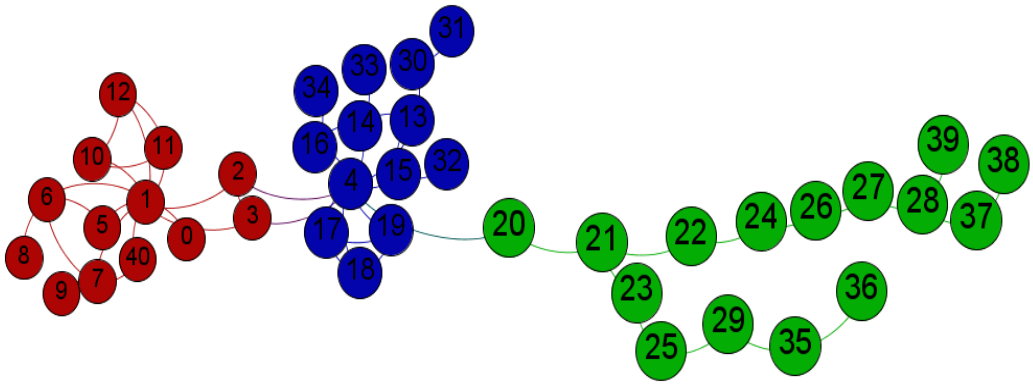


Figure 4.11 : Le graphe anonymisé à l'aide de l'algorithme **AnonSN**

Nous remarquons d'après le graphe anonymisé avec l'algorithme de Zhou et Pei illustré dans la figure 4.10, que pendant la procédure d'anonymisation les sommets 39 et 1 qui ont une

distance initiale égale à 12 sont reliés et sont devenus dans la même communauté (illustrée en vert). Dans le graphe original montré dans la figure 4.9, ils étaient dans deux communautés différentes, le sommet 1 dans la communauté montrée à droite en rouge et le 39 dans la communauté à gauche montrée en bleu. Par contre dans le graphe anonymisé produit par l'algorithme « AnonSN » illustré dans la figure 4.11, en ajoutant le faux sommet 40 au voisinage du sommet 1 (communauté décrite en rouge), les différents sommets restent dans leurs communautés initiales.

5.5 Mesures d'évaluation

Dans notre étude, nous considérons comme mesures d'utilité, les propriétés structurelles, en particulier les propriétés qui ont une relation avec la propriété de la distance qui sont les suivantes : « la longueur moyenne de chemins ou APL », « le diamètre », le « rayon », « le degré moyen » et « la densité de graphe ». Nous avons effectué deux expériences pour comparer l'algorithme existant de Zhou et Pei avec notre algorithme proposé « AnonSN ». Notre première expérience mesure et compare les différentes propriétés structurelles avant et après anonymisation. La deuxième expérience mesure les changements de la propriété « APL » ou le taux de distorsion de cette propriété selon plusieurs valeurs de k.

5.5.1 Première expérience : comparaison avec le modèle de référence selon les propriétés structurelles

Afin d'évaluer l'efficacité de l'approche proposée, nous calculons un certain nombre de mesures d'analyse de réseau social sur le graphe anonymisé G' produit à l'aide de l'algorithme de Zhou et Pei ainsi que sur le graphe anonymisé G'' produit par notre algorithme « AnonSN ». Ensuite, nous comparons ces mesures avec les mesures correspondantes au graphe original G. Le graphe anonymisé qui fournit des mesures plus proches de celles du graphe original est intuitivement plus utile pour l'analyse. La procédure des tests effectués sur les jeux de données se déroule selon le schéma suivant :

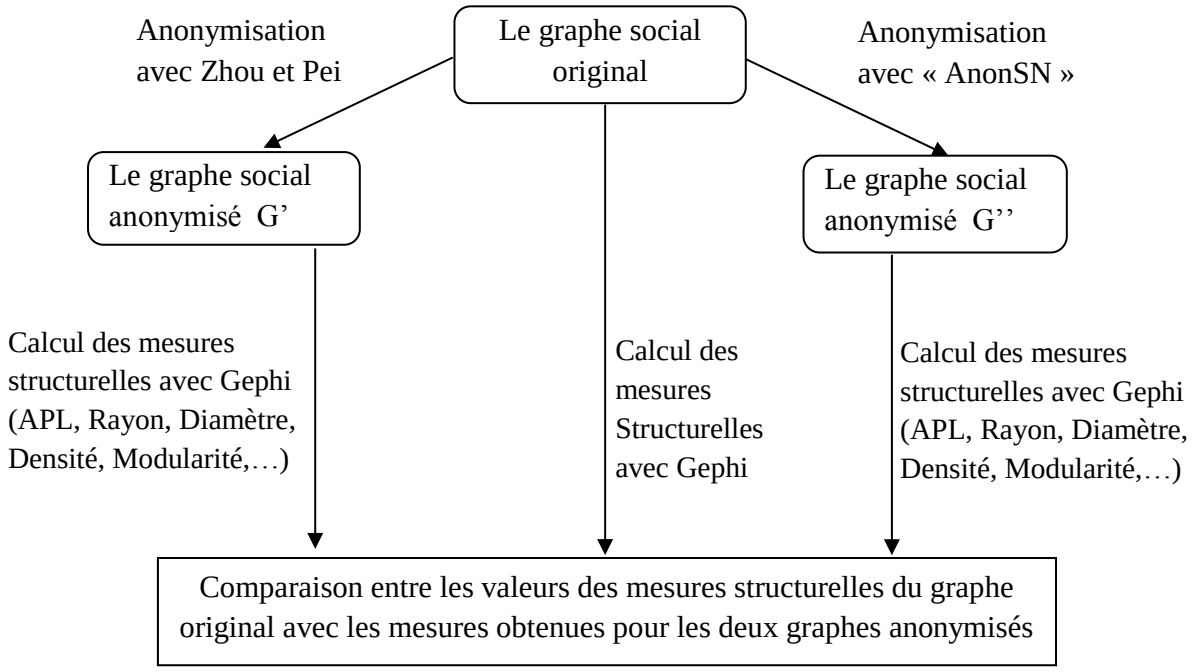


Figure 4.12 : Schéma des tests effectués

Nous avons divisé notre expérience en plusieurs étapes. Dans la première étape, nous prenons chaque graphe social original (synthétique ou réel) décrit précédemment à part, ce graphe sera d'abord anonymisé en utilisant l'algorithme de Zhou et Pei. Ensuite, ce même graphe est anonymisé en utilisant notre algorithme « AnonSN ». Pour chaque ensemble de données, nous avons utilisé la valeur de k=2.

Dans la seconde étape, nous calculons les valeurs des propriétés structurelles pour le graphe original et les graphes anonymisés résultants. Pour calculer les valeurs de toutes les propriétés structurelles, nous utilisons le logiciel Gephi [24]. Enfin, pendant la dernière étape de notre expérience, nous comparons les valeurs des propriétés structurelles mesurées pour le graphe social original avec celles obtenues pour les graphes anonymisés. Les résultats obtenus sont présentés dans les tableaux 1-6. Sur chaque tableau, la ligne représente les valeurs d'une propriété structurelle dans le graphe original et celui anonymisé en utilisant les deux algorithmes. Le contexte est défini par le couple : (nombre de sommets, nombre d'arêtes). Nous analysons et nous discutons tous ces résultats.

a) Résultat de calcul des propriétés structurelles : (graphes synthétiques et réels)

	Graphe Original	**« Zhou & Pei »**	**«AnonSN»**
Contexte	(40,51)	(40,56)	(41,54)
Nb arêtes ajoutées	/	5	3
Nb faux sommets ajoutés	/	/	1
APL	5.347435	4.485897	5.332926
Diamètre	13	12	13
Rayon	7	7	7
Degré moyen	2,550	2,800	2,634
Densité	0,065	0,072	0,066

Table 1 : Propriétés structurelles des graphes anonymisés générés pour le graphe synthétique 40 nœuds

	Graphe Original	**« Zhou & Pei »**	**«AnonSN »**
Contexte	(345,355)	(345,374)	(359,374)
Nb arêtes ajoutées	/	19	19
Nb faux sommets ajoutés	/	/	14
APL	5.061038	4.750640	5.007765
Diamètre	14	13	14
Rayon	7	7	7
Degré moyen	2,058	2,168	2,084
Densité	0,006	0,006	0,006

Table 2 : Propriétés structurelles des graphes anonymisés générés pour le graphe synthétique 345 nœuds

	Graphe Original	« Zhou & Pei »	«AnonSN »
Contexte	(1583,4212)	(1583,4358)	(1619,4358)
Nb arêtes ajoutées	/	146	146
Nb faux sommets ajoutés	/	/	36
APL	3.360509	3.204307	3.335308
Diamètre	6	6	6
Rayon	3	3	3
Degré moyen	5,322	5,506	5,384
Densité	0,003	0,003	0,003

Table 3 : Propriétés structurelles des graphes anonymisés générés pour le graphe réel « Enron_1583 »

	Graphe Original	« Zhou & Pei »	«AnonSN »
Contexte	(2086,35605)	(2086,36089)	(2128,36093)
Nb arêtes ajoutées	/	484	488
Nb faux sommets ajoutés	/	/	42
APL	2.80117	2.54512	2.78805
Diamètre	6	5	6
Rayon	3	3	3
Degré moyen	34.137	34,601	33,922
Densité	0,016	0,017	0,016

Table 4 : Propriétés structurelles des graphes anonymisés générés pour le graphe réel « Talk_presence » 2086 nœuds

	Graphe Original	« Zhou & Pei »	«AnonSN »
Contexte	(2579,6467)	(2579,6783)	(2638,6783)
Nb arêtes ajoutées	/	316	316
Nb faux sommets ajoutés	/	/	59
APL	3.406402	3.249174	3.383580
Diamètre	6	6	6
Rayon	3	3	3
Degré moyen	5,015	5,260	5,143
Densité	0,002	0,002	0,002

Table 5 : Propriétés structurelles des graphes anonymisés générés pour le graphe « Enron_2579 »

	Graphe Original	« Zhou & Pei »	«AnonSN »
Contexte	(3200,6267)	(3200,6951)	(3310,6951)
Nb arêtes ajoutées	/	684	684
Nb faux sommets ajoutés	/	/	110
APL	3.542312	3.375090	3.512778
Diamètre	4	4	5
Rayon	2	2	3
Degré moyen	3,917	4,344	4,200
Densité	0,001	0,001	0,001

Table 6 : Propriétés structurelles des graphes anonymisés générés pour le graphe « Enron_3200 »

b) Analyse des résultats obtenus

Nous pouvons remarquer d'après les tableaux que la valeur de la propriété APL calculée pour le graphe social anonymisé à l'aide de notre outil « AnonSN » est toujours plus proche de sa valeur calculée pour le graphe social original, donc elle est préservée.
Puisque par définition la propriété APL représente la distance moyenne entre les différents sommets du graphe et dans notre travail nous préservons toujours la distance moyenne entre le sommet dont le voisinage à anonymiser et le reste des sommets du graphe, alors la valeur d'APL est toujours préservée. Dans l'histogramme ci-dessous, nous illustrons les valeurs de cette propriété pour les 7 ensembles de données déjà définis dans la section 5.3 (ensembles de données réelles et synthétiques).

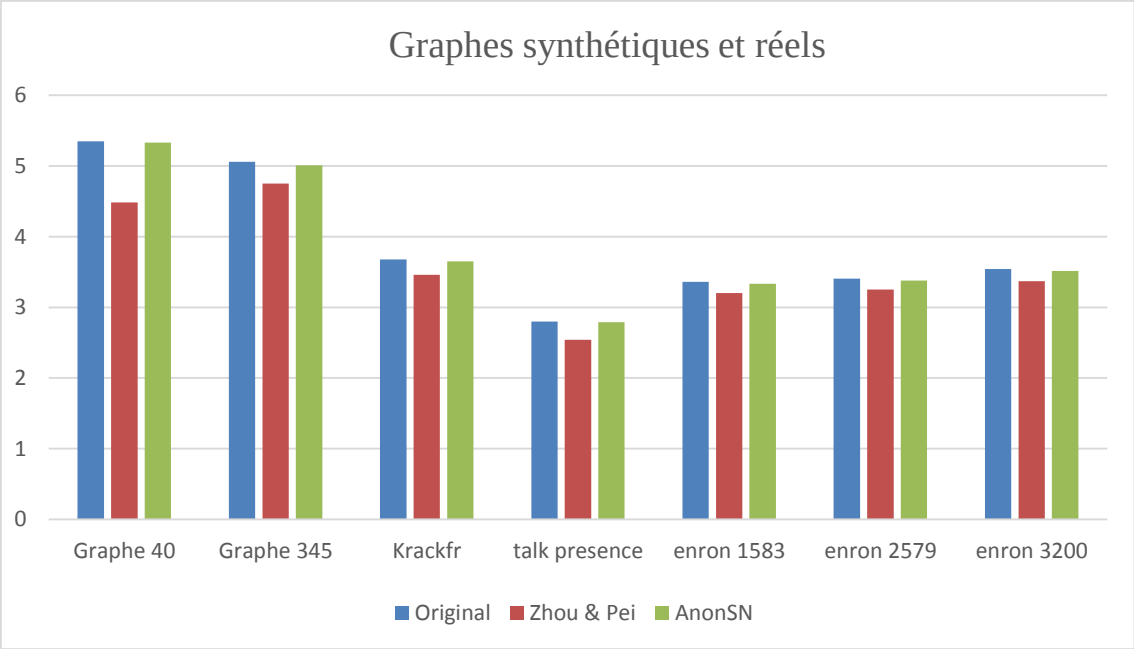


Figure 4.13 : APL pour différents ensembles de données étudiés avec k = 2

Selon la figure 4.13 ci-dessus, sur tous les ensembles de données anonymisés d'Enron et les autres ensembles de données, les valeurs de la mesure d'APL sur les graphes anonymisés à l'aide de notre algorithme « AnonSN » sont très proches de celles des graphes originaux. Les chiffres montrent également que cette propriété est mieux préservée à l'aide de notre algorithme que ce soit pour les petits graphes comme pour les grands graphes.

Pour les autres propriétés structurelles, leurs valeurs changent selon la structure des graphes utilisés dans les tests :

- Le diamètre, par définition représente la maximale de l'excentricité. La préservation de la distance moyenne ne signifie pas que la distance maximale est aussi préservée. Autrement dit, l'ajout de liens ou de faux sommets ne considère pas la distance maximale entre les différents sommets du graphe mais seulement la distance moyenne entre le sommet dont le voisinage à anonymiser et le reste des sommets du graphe. Dans le cas du graphe anonymisé à l'aide de l'algorithme de Zhou et Pei la valeur du diamètre diminue ou reste préservée, car l'ajout des liens diminue les distances surtout si les liens ajoutés relient des sommets lointains. Dans le cas de l'algorithme

« AnonSN », sa valeur reste préservée ou augmente, cela dépend de la position des faux nœuds ajoutés.

- Le rayon, par définition représente la minimale de l'excentricité de tous les nœuds du graphe. De la même manière, la préservation de la distance moyenne ne signifie pas que la distance minimale est aussi préservée. Dans le cas d'anonymisation à l'aide de l'algorithme de Zhou et Pei, sa valeur diminue ou reste préservée car l'ajout des liens diminue les distances, mais comme l'excentricité d'un sommet représente la maximale des distances avec le reste des sommets, dans certain cas même en ajoutant des liens entre un sommet u et d'autres sommets du graphe la valeur de l'excentricité de u reste préservée, et si pour chacun des sommets du graphe leur excentricité reste préservée alors la valeur du rayon reste aussi préservée, mais dans le cas où il y'a beaucoup d'arêtes ajoutées surtout si elles sont ajoutées entre des sommets lointains, les valeurs des distances diminuent, et ainsi les valeurs de l'excentricité des différents sommets diminuent, et par conséquent la valeur du rayon diminue également. Dans le cas de l'algorithme « AnonSN », la valeur du rayon reste préservée ou augmente, ceci dépend toujours de la position des faux sommets ajoutés.

- Pour la densité, elle dépend du nombre d'arêtes et de faux sommets ajoutés dans le graphe original.

Nous concluons, que notre algorithme « AnonSN » a pu préserver la valeur d'APL, et dans certains cas les valeurs d'autres propriétés structurelles basées sur la distance.

5.5.2 Deuxième expérience : Comparaison avec le modèle de référence selon les valeurs de k

a) Analyse de la variation d'APL selon k

Dans cette section, nous étudions les performances de l'approche proposée par rapport au modèle de référence de Zhou et Pei en fonction de différentes valeurs du paramètre d'anonymat « k ». La table 7 présente les résultats de calcul des valeurs de la propriété APL du graphe « Interest_434 » et ses graphes anonymisés à l'aide des deux algorithmes. Nous examinons ces résultats.

La figure 4.14 montre le processus de changement de la valeur d'APL du graphe « Interest_434 » selon différentes valeurs de k. L'axe vertical représente la valeur d'APL avant et après anonymisation, et l'axe horizontal représente la variation du paramètre d'anonymat k. La diminution de la valeur d'APL est dû à : plus le nombre de liens ajoutés entre les nœuds du graphe est grand plus la distance entre les nœuds diminue.

Nous remarquons d'après les graphiques que quel que soit la valeur de k, la valeur de l'APL du graphe anonymisé utilisant notre algorithme « AnonSN » est plus proche de sa valeur pour le graphe social original par rapport à l'algorithme existant. Quand $k \geq 3$, les valeurs de l'APL utilisant l'algorithme existant de Zhou et Pei changent beaucoup par rapport à celles avec « AnonSN ». Nous avons conclu que ceci se produit en raison de deux facteurs:

- Le nombre de nœuds à anonymiser ensemble augmente selon la valeur de k. Cela implique que le nombre d'arêtes à ajouter augmente. Par conséquent, plus d'arêtes seront ajoutées lors de l'exécution de l'algorithme sur certaines composantes de

voisinages, plus ceci conduit à la diminution de la distance moyenne entre les différents sommets, surtout pour l'algorithme de Zhou et Pei, où ils existent des cas où il relie des sommets lointains, ce qui diminue considérablement la distance.

- Pour l'algorithme « AnonSN », il sélectionne les nœuds les plus proches au nœud dont le voisinage à anonymiser, indépendamment de k. En plus, il y a des cas dans lesquels l'algorithme choisit d'ajouter des faux nœuds à la composante à anonymiser si ceci préserve mieux la distance moyenne originale.

		k=2	k=3	k=4	k=5
Contexte	Original	(434,1924)	(434,1924)	(434,1924)	(434,1924)
	Zhou&Pei	(434,2000)	(434,2101)	434,2096)	(434,2200)
	AnonSN	(442,2000)	(449,2101)	(451,2096)	(469,2211)
Nombre d'arêtes ajoutées	Zhou & Pei	76	177	172	276
	AnonSN	76	177	172	287
Nb faux sommets ajoutés	Zhou & Pei	/	/	/	/
	AnonSN	8	15	17	35
APL	Original	2.42296271857	2.42296271857	2.42296271857	2.42296271857
	Zhou & Pei	2.34258894647	2.28337288875	2.28313874905	2.24903949510
	AnonSN	2.374447214783	2.370367806018	2.40149051490	2.398155741439

Table 7 : valeurs de la propriété APL du graphe « Interest_434 » selon différente valeurs de k

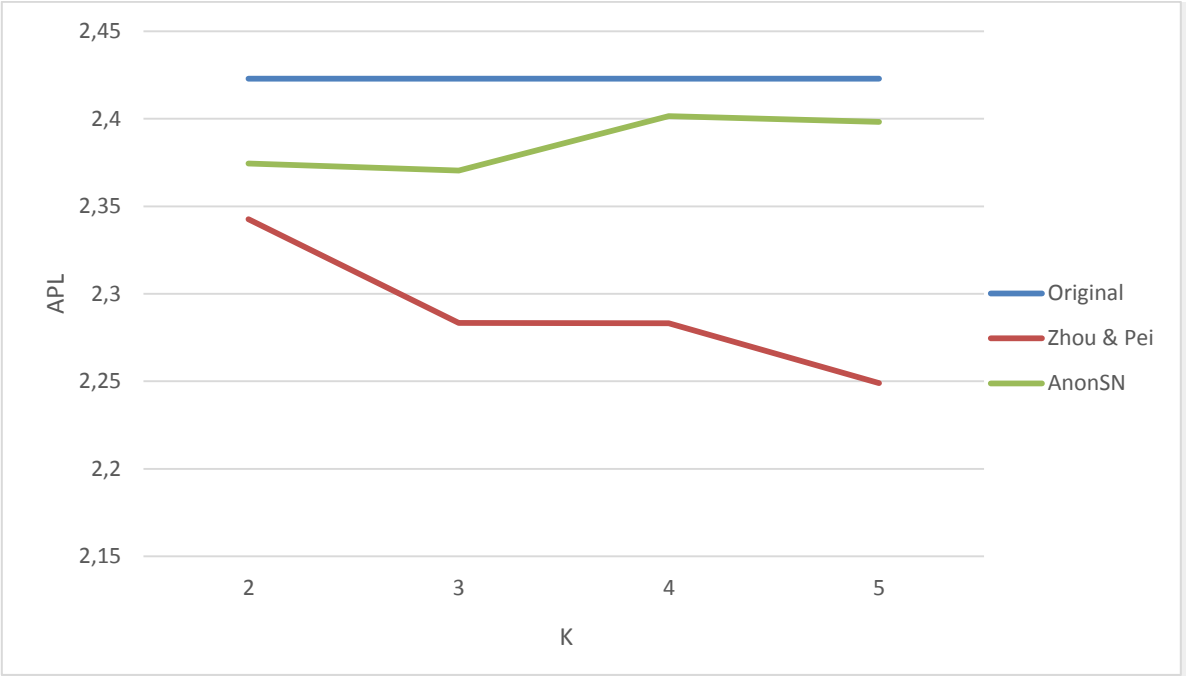


Figure 4.14 : Valeurs d'APL en fonction de k

b) La perte de l'information ou l'utilité du graphe anonymisé selon APL

Pour évaluer l'utilité du graphe anonymisé selon certaine mesure nous devons comparer la valeur de cette mesure pour le graphe anonymisé et le graphe original, la table 8 présente les différentes valeurs de la propriété APL correspondants au graphe «Krackfr_271» et ses graphes anonymisés générés selon différentes valeurs de k. L'utilité est représentée graphiquement comme **la distorsion** de la mesure calculée entre le graphe anonymisé et le graphe original. La figure 4.15 résume les résultats que nous avons obtenus pour la mesure d'utilité « APL » pour le graphe « Krackfr_271». L'axe horizontal montre les différentes valeurs de « k » (2, 5, 10, et 15) et l'axe vertical représente la distorsion. Les lignes représentent combien l'utilité du graphe anonymisé écarte de l'utilité du graphe original lorsque le graphe satisfait le k-anonymat. Dans la figure, la ligne en rouge correspond à l'algorithme de référence tandis que la ligne en vert représente les résultats de l'approche proposée. Les graphiques illustrent la performance de l'approche proposée par rapport le modèle de référence quel que soit la valeur de k. Une valeur de k plus élevée représente des exigences de confidentialité ou de vie privée plus élevées.

Nous analysons une propriété très importante - la longueur de chemins moyenne - (Average path length, ou APL) comme déjà définie dans le chapitre 3, elle représente la distance moyenne entre toutes les paires de sommets dans le réseau, ce qui reflète l'interdépendance d'un réseau. Par définition, APL sur un graphe G est exprimé comme suit :

$$APL_G = \frac{2}{N(N-1)} \sum_{\forall\, i,j \in G} d(i,j)$$

Où d(i,j) est la longueur du chemin le plus court entre les nœuds i et j, N est le nombre de nœuds dans le graphe.

La figure présente la comparaison de l'utilité de l'ensemble de données en termes d'« APL ». Les résultats montrent que la méthode proposée améliore considérablement la préservation de l'utilité. Comme prévu, le taux de distorsion pour cette mesure d'utilité augmente lorsque la valeur de k augmente, tandis que il n'y a pas une grande différence entre l'algorithme de référence et l'approche proposée quand k est petit parce que la quantité de modification est relativement petite.

Pour calculer le pourcentage de distorsion, nous avons utilisé la formule suivante :
$(|a-b|/\ a) \times 100$, où a est la valeur de la mesure pour le graphe anonymisé, et b est la valeur de la mesure pour le graphe original. La table 9 présente les valeurs de distorsion calculées en fonction du paramètre k entre le graphe « Krackfr_271 » et ses graphes anonymisés générés avec les deux algorithmes. Par exemple, les valeurs de « APL » quand k= 10 sont :

Originale = 3,678392783927839,
Modèle de référence = 3,4693180265135983,
La nôtre = 3,6492962387610035.

Alors nous obtenons : |3,4693180265135983-3,678392783927839| / 3,678392783927839x 100 = **5,68%,** et |3,6492962387610035- 3,678392783927839|/3,678392783927839x 100 = **0,79%,** le taux de distorsion pour le modèle de référence et notre approche respectivement. Par conséquent, l'approche proposée a 4,89% moins de distorsion par rapport le modèle de référence avec k=10. Par conséquent, les résultats expérimentaux prouvent que l'approche proposée produit une petite perte d'utilité.

		k=2	k=5	k=10	k=15
Contexte	Original	(271,359)	(271,359)	(271,359)	(271,359)
	Zhou&Pei	(271,370)	(271,398)	(271,466)	(271,506)
	AnonSN	(274,370)	(284,439)	(292,487)	(314,682)
Nombre d'arêtes ajoutées	Zhou & Pei	11	39	107	147
	AnonSN	11	80	128	323
Nb faux sommets ajoutés	Zhou & Pei	/	/	/	/
	AnonSN	3	13	21	43
APL	Original	3,67839278392	3,67839278392	3,67839278392	3,6783927832
	Zhou & Pei	3,64969249692	3,59024190241	3,469318026513	3,38786387838
	AnonSN	3,668244164594	3,680635047031	3,649296238761	3,69980260819

Table 8 : valeurs de la propriété APL du graphe «Krackfr_271» selon différentes valeurs de k

APL original= 3,678392783927839

		K=2	K=5	K=10	K=15
Zhou & Pei	APL	3,64969249692 4969	3,59024190241 9024	3,46931802651 3 5983	3,38786387863 8 7865
	Taux de distorsion	0,8%	2,4%	5,68%	7,9%
AnonSN	APL	3,66824416459 4 5296	3,68063504703 1 3043	3,64929623876 1 0035	3,69980260881 9 5193
	Taux de distorsion	0,27%	0,06%	0,79%	0,58%

Table 9 : Valeurs d'APL et son taux de distorsion pour le graphe « Krackfr_271» selon différentes valeurs de k

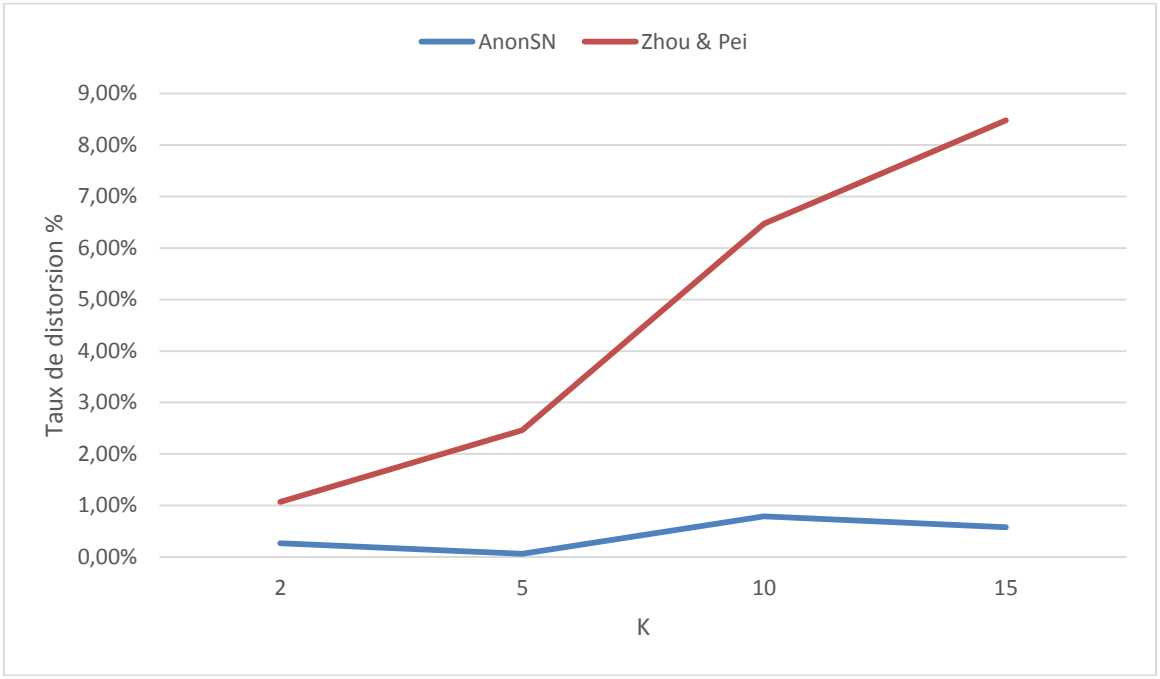


Figure 4.15 : taux de distorsion d'APL pour le graphe « Krackfr_271» selon différentes valeurs de k

6 Discussion et conclusion

Dans ce chapitre, nous avons présenté, et analysé les résultats de notre outil d'anonymisation « AnonSN » proposé qui considère la distance entre les nœuds comparativement à l'algorithme de Zhou et Pei [54]. Nous avons montré que notre outil donne des résultats satisfaisants selon les tests effectués, il permet de supprimer les changements des distances entre les nœuds et ainsi mieux préserver la propriété structurelle APL des graphes anonymisés, qui seront plus utiles pour l'analyse des données. Nos différents résultats expérimentaux démontrent que l'algorithme combinant l'ajout de faux nœuds avec l'ajout de liens peut obtenir de meilleurs résultats par rapport à celui basé seulement sur l'ajout de liens et il peut générer un graphe qui préserve efficacement la propriété APL.

1) Les résultats indiquent que notre algorithme préserve les distances moyennes par rapport à l'algorithme existant, parce que nous ajoutons des arêtes entre les nœuds les plus proches, et si cet ajout ne préserve pas la distance moyenne nous ajoutons des faux nœuds qui maintiennent ces distances proches de celles du graphe original.

2) La mesure de l'APL : Nous avons mesuré APL selon différentes valeurs du paramètre d'anonymat k pour confirmer si l'anonymisation pourrait éviter de dégrader l'exactitude des analyses en modifiant la distance entre les nœuds. Plus précisément, nous avons pour but de maintenir la valeur de l'APL dans un graphe anonymisé en le comparant à son graphe de réseau social original avant anonymisation car cela préserve l'utilité des données pour une analyse future, et nous avons pu atteindre cet objectif.

L'anonymisation d'un graphe est un processus nécessaire avant toute publication des données d'un réseau social afin de préserver la vie privée des individus du réseau. Plusieurs travaux ont été réalisés pour démontrer le risque de violation de la vie privée en publiant un graphe social naïvement anonymisé. Généralement, cette simple procédure n'est pas suffisante, et il est possible de ré-identifier certains individus dans le graphe social si l'adversaire possède certaines connaissances de base sur sa cible.

Tout au long de ce projet, notre travail consistait à étudier l'attaque de voisinage et de comprendre les approches existantes pour prévenir cette attaque, notamment l'algorithme proposé par Zhou et Pei [54], afin de proposer une nouvelle approche d'anonymisation des graphes sociaux. L'étude approfondie de cette approche nous a permis de déceler un ensemble de limites sur l'utilité du graphe anonymisé résultant, à savoir les propriétés structurelles du graphe qui sont altérées, ce qui nous a conduit à proposer un nouvel algorithme d'anonymisation. Ce dernier a pour but non seulement de prévenir la ré-identification des individus à travers l'information de « voisinage » mais aussi de préserver une propriété structurelle très importante du graphe à savoir : « APL ».

Pour proposer notre solution, il nous a fallu :

- Etudier le concept des réseaux sociaux et leur modélisation sous forme de graphes ainsi que les menaces de sécurité liées à la préservation de la vie privée des utilisateurs lors de la publication des données du réseau social.

- Etudier de manière détaillée l'approche d'anonymisation proposée par Zhou et Pei [54] ainsi que son amélioration par Tripathy et al [64] en utilisant les matrices d'adjacence pour prévenir l'attaque de voisinage.

- Identifier les limites des approches existantes : à l'issue de cette étape, nous avons pu identifier quelques faiblesses concernant la distorsion des propriétés structurelles du graphe anonymisé résultant.

Ainsi, nous avons proposé une nouvelle approche d'anonymisation du graphe social pour contrecarrer les faiblesses d'utilité, et nous avons pu développer un outil pour anonymiser le graphe représentant le réseau social à publier tout en maintenant l'utilité des données du réseau.
L'approche d'anonymisation proposée garantit que, pour toute modification apportée au graphe original, la propriété de distance moyenne entre les sommets impliqués est aussi proche que possible à celle dans le graphe original. Nous avons proposé également une nouvelle formule de calcul du coût d'anonymisation. En résumé, nous avons apporté les principales contributions suivantes:

1. Proposition d'une nouvelle formule de calcul du coût d'anonymisation pour déterminer les voisinages des sommets qui peuvent êtres anonymisés ensemble.

2. Proposition d'une nouvelle approche d'anonymisation basée sur l'ajout de faux nœuds en plus de l'ajout de liens.

3. Comparaison des résultats de l'approche proposée d'ajout de faux nœuds par rapport à l'approche de Zhou et Pei selon la préservation de l'APL et analyser l'influence des changements de la distance sur d'autres propriétés structurelles.

La méthode d'anonymisation proposée combine l'ajout de faux sommets avec l'ajout d'arêtes, et se déroule en deux étapes :

1. D'abord, nous extrayons les voisinages de tous les sommets dans le graphe. Pour faciliter les comparaisons entre les voisinages des différents sommets, y compris les tests d'isomorphisme qui sont fréquemment effectués dans l'anonymisation, nous représentons les différentes composantes de voisinage sous forme de matrices d'adjacence.

2. Dans la deuxième étape, nous organisons les sommets en groupes (avec des tailles d'au moins k) en se basant sur le coût d'anonymisation et nous procédons à l'anonymisation des voisinages des sommets dans le même groupe. L'anonymisation est basée sur l'ajout d'arêtes et l'ajout de faux nœuds dans le graphe original. Le choix entre l'ajout d'arêtes et l'ajout de faux sommets est conditionné par la préservation des distances moyennes entre les différents sommets sur laquelle se base d'autres propriétés structurelles. Dans cette étape, plusieurs algorithmes sont développés comme l'algorithme d'anonymisation de deux voisinages, l'algorithme de vérification et d'anonymisation de deux composantes de voisinage et l'algorithme de choix entre l'ajout de nœuds existant et l'ajout de faux nœuds.

Afin de maintenir l'utilité du graphe à publier, il est nécessaire d'ajouter le moins possible d'arêtes ainsi que de faux sommets.

Dans le but de comparer l'approche proposée avec celle de Zhou et Pei, il était nécessaire d'implémenter l'algorithme de Zhou et Pei, cette implémentation était difficile et a nécessité beaucoup d'effort à cause du manque de détails techniques dans la littérature.

Les différents tests réalisés sur une variété de données réelles et synthétiques générés nous ont permis de conclure que l'algorithme d'ajout de faux nœuds peut obtenir de meilleurs résultats et montre des améliorations significatives dans le maintien de l'APL par rapport aux travaux précédents qui se basent sur l'ajout de liens seulement.

A l'issue de ce travail, des extensions et perspectives futures sont envisagées pour l'améliorer, à savoir:

- Traiter le cas de d >1, c'est à dire lorsque l'adversaire a des connaissances de base sur les voisins de la victime à d sauts.

- Il serait intéressant de réduire le nombre de faux nœuds ajoutés, autrement dit étudier le nombre de faux sommets ajoutés par rapport :

  - au nombre de sommets original total
  - à la nature de graphe social à anonymiser

- Nous prévoyons aussi d'étudier d'autres propriétés structurelles de réseau afin d'améliorer encore la préservation de l'utilité dans l'anonymisation de réseau social.

- Une autre direction intéressante est de considérer la mise en œuvre de ce modèle dans un graphe avec labels sensibles en introduisant le concept de « l-diversité » pour prévenir les attaques d'homogénéité et mieux protéger les labels sensibles tout en préservant les propriétés structurelles.

[1]: BACHELET, Rémi. Réseaux sociaux. Cour distribué sous licence Creative Commons. 2014. http://rb.ec-lille.fr/l/Socio_orgas/cours-socio_reseaux_sociaux.pdf

[2]: MIKA, Peter. Ontologies are us: A unified model of social networks and semantics. In : *The Semantic Web–ISWC 2005*. Springer Berlin Heidelberg, 2005. p. 522-536.

[3]: WELLMAN, Barry. Computer networks as social networks. Science, 2001, vol. 293, no 5537, p. 2031-2034.

[4]: CAVAZZA, Frédéric. Social Media Landscape: http://www.fredcavazza.net/2015/05/29/panorama-des-medias-sociaux-2015/ (vu le 15/06/2015)

[5] : RUSHED, Kanawati , ROUVEIROL, Céline. Prédiction de liens dans les réseaux sociaux, Tutoriel EGC, 2010

[6] : ERÉTÉO, Guillaume, GANDO, F., BUFFA, M., et al. Analyse des réseaux sociaux et web sémantique: un état de l'art. Projet: Intégration sémantique de l'information par des communautés d'intelligence en ligne, ANR, 2009.

[7] : Christophe ROSSIGNOL, Graphes pondérés, Graphes étiquetés, Graphes probabilistes, cour placé sous licence Creative Commons BY-SA http://creativecommons.org/licenses/by-sa/2.0/fr/, 2009

[8]: ELLISON, Nicole B., *et al.* Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 2007, vol. 13, no 1, p. 210-230.

[9]: LI, Ninghui, LI, Tiancheng, et VENKATASUBRAMANIAN, Suresh. t-closeness: Privacy beyond k-anonymity and l-diversity. In : *Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on*. IEEE, 2007. p. 106-115.

[10]: JY Bodin. Réseaux sociaux et e-collecte : quelle stratégie web pour les organisations caritatives ? . Master 2 Web éditorial – 2011

[11]: HO, Ai Thanh. Towards a Privacy-Enhanced Social Networking Site. 2012.

[12] : RAUX, Stéphane. Dynamiques des réseaux sociaux en ligne.

[13]: FANG, Binxing, JIA, Yan, HAN, Yi, *et al.* A survey of social network and information dissemination analysis. *Chinese science bulletin*, 2014, vol. 59, no 32, p. 4163-4172.

[14]: HAFEZ, Ahmed Ibrahem, HASSANIEN, Aboul Ella, et FAHMY, Aly A. Testing community detection algorithms: A closer look at datasets. In : *Social Networking*. Springer International Publishing, 2014. p. 85-99.

[15] : http://www.digitalbuzzblog.com/slideshare-fortune-100-social-media-statistics-2012/ (vu le 15/03/2014)

[16] : http://www.blogdumoderateur.com/chiffres-facebook/ (vu le 20/11/2015)

[17] : BEAUGUITTE, Laurent et MERCKLÉ, Pierre. Analyse des réseaux: Une introduction à Pajek.

[18]: SORYANI, Mohammad et MINAEI, Behrooz. Social Networks Research Aspects: A Vast and Fast Survey Focused on the Issue of Privacy in Social Network Sites. *arXiv preprint arXiv:1201.3745*, 2012.

[19] : LEBHAR, Emmanuelle. *Algorithmes de routage et modèles aléatoires pour les graphes petits mondes*. 2005. Thèse de doctorat. Ecole normale supérieure de lyon-ENS LYON.

[20] : MILGRAM, Stanley. The small world problem. *Psychology today*, 1967, vol. 2, no 1, p. 60-67.

[21] : FALOUTSOS, Michalis, FALOUTSOS, Petros, et FALOUTSOS, Christos. On power-law relationships of the Internet topology. In : *ACM SIGCOMM computer communication review*. ACM, 1999. p. 251-262.

[22] : GUILLAUME, Jean-Loup. *Analyse statistique et modélisation des grands réseaux d'interactions*. 2004. Thèse de doctorat. Université Paris-Diderot-Paris VII.

[23]: SCOTT, John. *Social network analysis*. Sage, 2012.

[24]: WASSERMAN, Stanley et FAUST, Katherine. *Social network analysis: Methods and applications*. Cambridge university press, 1994.

[25]: SINGH, Amardeep, BANSAL, Divya, et SOFAT, Sanjeev. Privacy Preserving Techniques in Social Networks Data Publishing-A Review. International Journal of Computer Applications, 2014, vol. 87, no 15.

[26] : JIANG, Yichuan et JIANG, J. C. Understanding social networks from a multiagent perspective. *Parallel and Distributed Systems, IEEE Transactions on*, 2014, vol. 25, no 10, p. 2743-2759.

[27]: SAMARATI, Pierangela. Protecting respondents identities in microdata release. *Knowledge and Data Engineering, IEEE Transactions on*, 2001, vol. 13, no 6, p. 1010-1027.

[28]: HANNEMAN, Robert A. et RIDDLE, Mark. Introduction to social network methods. 2005.

[29]: HOGBEN, Giles. Security issues and recommendations for online social networks. *ENISA position paper*, 2007, vol. 1, p. 1-36.

[30] : SADEGHIAN, Alireza, ZAMANI, Mahdi, et SHANMUGAM, Bharanidharan. Security threats in online social networks. In : *Informatics and Creative Multimedia (ICICM), 2013 International Conference on*. IEEE, 2013. p. 254-258.

[31] : ANSARI, Fazel, AKHLAQ, Monis, et RAUF, Abdul Mannan. Social networks and web security: Implications on open source intelligence. In : *Information Assurance (NCIA), 2013 2nd National Conference on*. IEEE, 2013. p. 79-82.

[32]: ZHOU, Bin, PEI, Jian, et LUK, WoShun. A brief survey on anonymization techniques for privacy preserving publishing of social network data. *ACM Sigkdd Explorations Newsletter*, 2008, vol. 10, no 2, p. 12-22.

[33] GRIER, Chris, THOMAS, Kurt, PAXSON, Vern, *et al.* @ spam: the underground on 140 characters or less. In : *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010. p. 27-37.

[34] : SEIFI, Massoud. *Cœurs stables de communautés dans les graphes de terrain*. 2012. Thèse de doctorat.

[35] : GRABOWICZ, Przemyslaw Adam, *et al.* Complex networks approach to modeling online social systems. The emergence of computational social science. 2014.

[36]: LEVALLOIS, Clément. Gephi – les fondations, V 1.0 – Nov. 2013.

[37]: RICHARDSON, Matthew et DOMINGOS, Pedro. Mining knowledge-sharing sites for viral marketing. In : *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2002. p. 61-70.

[38]:https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social (vu le 01/05/2014)

[39] : Facebook " Paramètres de confidentialité des applications et de vos informations" https://www.facebook.com/help/262314300536014 (vu le 02/10/2014)

[40]: SHARMA, Sanur, GUPTA, Preeti, et BHATNAGAR, Vishal. Anonymisation in social network: a literature survey and classification. International Journal of Social Network Mining, 2012, vol. 1, no 1, p. 51-66.

[41]: SALAMA, Mostafa, PANDA, Mrutyunjaya, ELBARAWY, Yomna, *et al.*Computational Social Networks: Security and Privacy. In : *Computational Social Networks*. Springer London, 2012. p. 3-21.

[42]: GHESMOUNE, Mohammed. Anonymisation de réseaux sociaux. 2012.

[43]: KAPLAN, Andreas M. et HAENLEIN, Michael. Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, 2010, vol. 53, no 1, p. 59-68.

[44]:http://tpe-individualisation-adolescents.e-monsite.com/pages/la-definition-des-reseaux-sociaux.html (vu le 01/01/2015)

[45] : http://mrvar.fdv.uni-lj.si/pajek/ (vu le 10/10/2015)

[46]: BALSA, E. *DummySN: Privacy-preserving social networks*. 2010. Thèse de doctorat. Master's thesis, Katholieke Universiteit Leuven, Belgium.

[47]: BACKSTROM, Lars, DWORK, Cynthia, et KLEINBERG, Jon. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In : *Proceedings of the 16th international conference on World Wide Web*. ACM, 2007. p. 181-190.

[48]: HAY, Michael, MIKLAU, Gerome, JENSEN, David, *et al.* Resisting structural re-identification in anonymized social networks. *Proceedings of the VLDB Endowment*, 2008, vol. 1, no 1, p. 102-114.

[49]: CHBEIR, Richard et AL BOUNA, Bechara. Security and privacy preserving in social networks. Springer, 2013.

[50]: ZHANG, Lijie et ZHANG, Weining. Edge anonymity in social network graphs. In : *Computational Science and Engineering, 2009. CSE'09. International Conference on*. IEEE, 2009. p. 1-8.

[51]: ZHANG, Lijie et ZHANG, Weining. Privacy Protection of Social Network Graphs, 2011.

[52]: WONDRACEK, Gilbert, HOLZ, Thorsten, KIRDA, Engin, et al. A practical attack to de-anonymize social network users. In : Security and Privacy (SP), 2010 IEEE Symposium on. IEEE, 2010. p. 223-238.

[53]: LIU, Kun et TERZI, Evimaria. Towards identity anonymization on graphs. In : Proceedings of the 2008 ACM SIGMOD international conference on Management of data. ACM, 2008. p. 93-106.

[54]: ZHOU, Bin et PEI, Jian. Preserving privacy in social networks against neighborhood attacks. In : Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on. IEEE, 2008. p. 506-515.

[55]: YING, Xiaowei et WU, Xintao. Randomizing Social Networks: a Spectrum Preserving Approach. In : SDM. 2008. p. 739-750.

[56]: Sharma, D. (2007). Social networking god: 350+ social networking sites. http://mashable.com/2007/10/23/social-networking-god/ (vu le 01/05/2014).

[57] : INITIATION AU LANGAGE JAVA, http://docplayer.fr/2810688-Initiation-au-langage-java.html (vu le 05/05/2015)

[58]: NARAYANAN, Arvind et SHMATIKOV, Vitaly. De-anonymizing social networks. In : Security and Privacy, 2009 30th IEEE Symposium on. IEEE, 2009. p. 173-187.

[59] : BHAGAT, Smriti, CORMODE, Graham, SRIVASTAVA, Divesh, et al. Prediction Promotes Privacy in Dynamic Social Networks. In : WOSN. 2010.

[60]: LIU, Kun, DAS, Kamalika, GRANDISON, Tyrone, et al. Privacy-preserving data analysis on graphs and social networks. 2008.

[61]: ZHELEVA, Elena et GETOOR, Lise. Preserving the privacy of sensitive relationships in graph data. In : Privacy, security, and trust in KDD. Springer Berlin Heidelberg, 2008. p. 153-171.

[62]: HAY, Michael, MIKLAU, Gerome, JENSEN, David, et al. Anonymizing social networks. Computer science department faculty publication series, 2007, p. 180.

[63] : ZOU, Lei, CHEN, Lei, et ÖZSU, M. Tamer. K-automorphism: A general framework for privacy preserving network publication. Proceedings of the VLDB Endowment, 2009, vol. 2, no 1, p. 946-957.

[64]: TRIPATHY, B. K. et PANDA, G. K. A new approach to manage security against neighborhood attacks in social networks. In : Advances in Social Networks Analysis and Mining (ASONAM), 2010 International Conference on. IEEE, 2010. p. 264-269.

[65]: BHAGAT, Smriti, CORMODE, Graham, KRISHNAMURTHY, Balachander, et al. Class-based graph anonymization for social network data. Proceedings of the VLDB Endowment, 2009, vol. 2, no 1, p. 766-777.

[66]: PANDA, G. K., MITRA, A., PRASAD, Ajay, *et al.* Applying l-diversity in anonymizing collaborative social network. *International Journal of Computer Science and Information Security*, 2010, vol. 8, no 2, p. 324-329.

[67]: Nations, D. (2007). The top social networking sites. http://webtrends.about.com/od/socialnetworking/a/social_network.htm (vu le 01/05/2014).

[68] : CORMODE, Graham, SRIVASTAVA, Divesh, YU, Ting, et al. Anonymizing bipartite graph data using safe groupings. Proceedings of the VLDB Endowment, 2008, vol. 1, no 1, p. 833-844.

[69] : CHENG, James, FU, Ada Wai-chee, et LIU, Jia. K-isomorphism: privacy preserving network publication against structural attacks. In : Proceedings of the 2010 ACM SIGMOD International Conference on Management of data. ACM, 2010. p. 459-470.

[70] : MAO, Huina, SHUAI, Xin, et KAPADIA, Apu. Loose tweets: an analysis of privacy leaks on twitter. In : Proceedings of the 10th annual ACM workshop on Privacy in the electronic society. ACM, 2011. p. 1-12.

[71]: LI, Na et DAS, Sajal K. Applications of k-Anonymity and ℓ-Diversity in Publishing Online Social Networks. Springer New York, 2013.

[72]: HEATHERLY, Raymond, KANTARCIOGLU, Murat, et THURAISINGHAM, Bhavani. Preventing private information inference attacks on social networks. Knowledge and Data Engineering, IEEE Transactions on, 2013, vol. 25, no 8, p. 1849-1862.

[73]: GÜRSES, Seda, *et al.* SPION D2. 1-State of the Art. *SBO Security and Privacy for Online Social Networks*, 2011.

[74] : LI, Na, ZHANG, Nan, et DAS, Sajal K. Relationship privacy preservation in publishing online social networks. In : *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third*

Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on. IEEE, 2011. p. 443-450.

[75]: LI, Na, ZHANG, Nan, et DAS, Sajal K. Relationship privacy preservation in publishing online social networks. In : Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on. IEEE, 2011. p. 443-450.

[76]: MACHANAVAJJHALA, Ashwin, KIFER, Daniel, GEHRKE, Johannes, *et al.* l-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 2007, vol. 1, no 1, p. 3.

[77] : LAN, Lihui, JIN, Hua, et LU, Yang. Personalized anonymity in social networks data publication. In : Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on. IEEE, 2011. p. 479-482.

[78]: ZHOU, Bin et PEI, Jian. The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks. Knowledge and Information Systems, 2011, vol. 28, no 1, p. 47-77.

[79]: YUAN, Mingxuan, CHEN, Lei, YU, Philip S., et al. Protecting sensitive labels in social network data anonymization. Knowledge and Data Engineering, IEEE Transactions on, 2013, vol. 25, no 3, p. 633-647.

[80] : HONGWEI, Wu, JIANPEI, Zhang, BO, Wang, et al. (d, k)-Anonymity for Social Networks Publication against Neighborhood Attacks. Journal of Convergence Information Technology, 2013, vol. 8, no 2.

[81] : JIAO, Jia, LIU, Peng, et LI, Xianxian. A Personalized Privacy Preserving Method for Publishing Social Network Data. In : Theory and Applications of Models of Computation. Springer International Publishing, 2014. p. 141-157.

[82] : MISLOVE, Alan, MARCON, Massimiliano, GUMMADI, Krishna P., *et al.*Measurement and analysis of online social networks. In : *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*. ACM, 2007. p. 29-42.

[83] : XIAO, Xiaokui et TAO, Yufei. Output perturbation with query relaxation. Proceedings of the VLDB Endowment, 2008, vol. 1, no 1, p. 857-869.

[84]: FONG, Philip WL. Preventing sybil attacks by privilege attenuation: A design principle for social network systems. In : Security and privacy (SP), 2011 IEEE symposium on. IEEE, 2011. p. 263-278.

[85]: KRACKHARDT, David. Cognitive social structures. *Social networks*, 1987, vol. 9, no 2, p. 109-134.

[86]: SWEENEY, Latanya. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 2002, vol. 10, no 05, p. 557-570.

[87]: SAMARATI, Pierangela et SWEENEY, Latanya. *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression*. Technical report, SRI International, 1998.

[88] :http://master-iesc-angers.com/utilisation-du-logiciel-gephi-pour-lanalyse-cartographique/ (Vu le 01/09/2015)

[89]: TAYI, Giri Kumar et BALLOU, Donald P. Examining data quality. Communications of the ACM, 1998, vol. 41, no 2, p. 54-57.

[90]: BHAGAT, Smriti, CORMODE, Graham, KRISHNAMURTHY, Balachander, et al. Privacy in dynamic social networks. In : Proceedings of the 19th international conference on World wide web. ACM, 2010. p. 1059-1060.

[91]: WESTIN, Alan F. Privacy and freedom. *Washington and Lee Law Review*, 1968, vol. 25, no 1, p. 166.

[92]: ZHELEVA, Elena et GETOOR, Lise. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In : Proceedings of the 18th international conference on World wide web. ACM, 2009. p. 531-540.

[93]: WATANABE, Chiemi, AMAGASA, Toshiyuki, et LIU, Ling. Privacy risks and countermeasures in publishing and mining social network data. In :*Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference on*. IEEE, 2011. p. 55-66.

[94]: WU, Xintao, YING, Xiaowei, LIU, Kun, *et al.* A survey of privacy-preservation of graphs and social networks. In : *Managing and mining graph data*. Springer US, 2010. p. 421-453.