Universidade Federal
do Rio de Janeiro
Escola Politécnica

PROPOSTA E AVALIAÇÃO DE UM ALGORITMO PARA PROMOVER ATAQUES DE QUEBRA DE PRIVACIDADE EM REDES ANONIMIZADAS

Pamela Tabak

Projeto de Graduação apresentado ao Curso de Computação e Informação da Escola Politécnica da Universidade Federal do Rio de Janeiro como parte dos requisitos necessários para a obtenção do grau de Engenheiro de Computação e Informação.

Orientador: Daniel Ratton Figueiredo

Rio de Janeiro
Julho de 2017

PROPOSTA E AVALIAÇÃO DE UM ALGORITMO PARA PROMOVER ATAQUES DE QUEBRA DE PRIVACIDADE EM REDES ANONIMIZADAS

Pamela Tabak

PROJETO SUBMETIDO AO CORPO DOCENTE DO CURSO DE COMPUTAÇÃO E INFORMAÇÃO DA ESCOLA POLITÉCNICA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ENGENHEIRO DE COMPUTAÇÃO E INFORMAÇÃO.

Examinadores:

Prof. Daniel Ratton Figueiredo, Dr.

RIO DE JANEIRO, RJ – BRASIL
JULHO DE 2017

Tabak, Pamela

Proposta e Avaliação de um Algoritmo para Promover Ataques de Quebra de Privacidade em Redes Anonimizadas/Pamela Tabak. – Rio de Janeiro: UFRJ/POLI – COPPE, 2017.

IX, 14 p.: il.; 29, 7cm.

Orientador: Daniel Ratton Figueiredo

Projeto (graduação) – UFRJ/ Escola Politécnica/ Curso de Computação e Informação, 2017.

Referências Bibliográficas: p. 14 – 14.

1. Grafos. 2. Redes Sociais. 3. Anonimização. 4. Privacidade em Mineração de Dados. 5. Redes Complexas. I. Figueiredo, Daniel Ratton. II. Universidade Federal do Rio de Janeiro, Escola Politécnica/ Curso de Computação e Informação. III. Título.

Agradecimentos

Agradeço aos meus pais, os engenheiros que sempre me incentivaram e forneceram todo o suporte para que eu pudesse estar aqui hoje.

Agradeço a todos os professores do curso, que me deram as ferramentas para me tornar engenheira.

Por fim, agradeço ao professor Daniel Figueiredo, por todos os ensinamentos ministrados ao longo da faculdade e pela disposição e motivação em dar aula e orientar este projeto.

Resumo do Projeto de Graduação apresentado à Escola Politécnica/COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Engenheiro de Computação e Informação.

PROPOSTA E AVALIAÇÃO DE UM ALGORITMO PARA PROMOVER ATAQUES DE QUEBRA DE PRIVACIDADE EM REDES ANONIMIZADAS

Pamela Tabak

Julho/2017

Orientador: Daniel Ratton Figueiredo

Curso: Engenharia de Computação e Informação

Palavras-Chave: Grafos, Redes Sociais, Anonimização, Privacidade em Mineração de Dados, Redes Complexas.

Abstract of the Undergraduate Project presented to Poli/COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Computer and Information Engineer.

PROPOSAL AND EVALUATION OF AN ALGORITHM TO PROMOTE PRIVACY BREACH IN ANONYMISED NETWORKS

Pamela Tabak

July/2017

Advisor: Daniel Ratton Figueiredo

Course: Computer and Information Engineering

Keywords: Graphs, Social Networks, Anonimization, Privacy in Data Mining, Complex Networks.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Os traços digitais da interação social humana são facilmente encontrados ao redor da Web. Sites com relações sociais entre seus usuários têm se tornado cada vez mais comuns e facilmente aceitos e usados pela população. Consequentemente, essas fontes se tornaram, nos últimos anos, dados importantes para estudos de larga escala de redes sociais.

Em muitas dessas fontes de interação social, a interação entre os usuários é pública, isto é, a informação que o usuário x está associado ao usuário y pode ser vista por qualquer usuário. Esse seria o caso do Facebook, por exemplo, em que as relações entre usuários podem ser vistas por qualquer um. Entretanto, existem muitas redes sociais em que essas relações não são disponibilizadas publicamente. Nelas, cada usuário conhece apenas aqueles aos quais ele está relacionado, que serão chamados de seus vizinhos ao longo deste trabalho. Isto é, cada usuário sabe seu grau, porém a única informação que eles podem assumir de seus vizinhos é que o grau deles é maior igual a 1. Um exemplo desse tipo de rede seria a de troca de e-mail: cada usuário sabe para quem ele já enviou e de quem ele já recebeu e-mails, porém ele não é capaz de saber se um usuário qualquer já enviou ou recebeu algum e-mail de outro usuário.

Neste trabalho, será analisada a seguinte situação: uma rede social anuncia que irá divulgar o grafo que representa as relações entre seus usuários, porém sem a identificação de cada usuário, de modo que entidades possam realizar estudos empíricos a partir dos dados divulgados ou ajudá-las nas resolução de problemas, se tornando uma situação comum. Um caso bem famoso foi o da Netflix, descrito em [1], que divulgou seus dados de usuários e filmes, anonimizados, de modo a criar uma competição entre pessoas do mundo inteiro para desenvolver um sistema de recomendação para a empresa que recomendasse filmes à usuários, sem conhecer a identidade desses usuários ou filmes.

Nesse contexto, a privacidade das informações anonimizadas divulgadas pode ser comprometida, por meio de diferentes tipos de ataques que podem ser realizados.

1.1 Tipos de Ataque

Nessa conjectura, existem algumas abordagens proeminentes [2]: ativo, passivo e híbrido.

1.1.1 Ativo

Ataques ativos são algoritmos em que o atacante escolhe um número arbitrário de usuários que ele deseja violar a privacidade, cria um número pequeno de novos usuários com arestas com os nós atacados e cria um padrão de arestas entre esses novos usuários de modo a criar um subgrafo de novos nós que se destaque na rede anonimizada.

Neste ataque, qualquer usuário da rede pode ser escolhido para ser atacado. Contudo, como ele altera a estrutura da rede, adicionando um novo subgrafo à rede inicial com características próprias, a detecção deste ataque pode ser feita. Isto é, o subgrafo de atacantes é adicionado sem qualquer conhecimento prévio sobre a rede ou suas métricas, de modo que se os administradores da rede realizarem checagens periódicas na mesma, podem, por exemplo, detectar uma mudança na distribuição de grau dos nós e, consequentemente, suspeitar de um possível ataque.

1.1.2 Passivo

Neste ataque, os atacantes são alguns dos próprios usuários do sistema a ser atacado. Eles não criam novos usuários ou novas arestas, usando a informação que eles possuem da rede, deles mesmos, para encontrá-los na rede anonimizada e, a partir disto, tentar descobrir arestas entre usuários a quem eles estão relacionados.

No ataque passivo, por sua vez, apenas usuários relacionados ao grupo de usuários atacantes podem ser atacados, limitando a informação que será extraída da rede. Entretanto, este ataque não altera a estrutura da rede, de modo que ele não possa ser detectado como um possível ataque.

1.1.3 Híbrido

O ataque híbrido, também conhecido por ataque semi-passivo, surgiu como uma forma de tentar mesclar as boas características dos ataques ativo e passivo, de forma a tentar diminuir, também, os efeitos ruins deles.

Neste ataque, os atacantes também são usuários do sistema. Eles não criam nenhum novo usuário, porém eles criam algumas novas arestas para os usuários atacados antes da rede ser divulgada, de forma a poder atacar qualquer usuário da rede.

1.2 Motivação

É inegável que as redes sociais se tornaram parte do cotidiano de muita gente. O Facebook, uma dos maiores exemplos do início do século XXI, chegou a 1.6 bilhão de usuários em 2016, cerca de metade da população mundial com acesso à internet.

Neste contexto, é cada vez mais incomum ver pessoas duvidarem da segurança de seus dados, o que fica evidente em qualquer pesquisa feita sobre a quantidade de pessoas que realmente leram os termos e condições de uso de uma rede social antes de assiná-lo, uma vez que se é prometido privacidade. A dúvida que resta tirar é: os dados realmente não podem ser comprometidos?

A privacidade em redes, e na Web em geral, continua sendo um assunto importante e muito comentado, entretanto. De tempos em tempos é possível ver no noticiário grandes empresas que tiveram parte de seus dados hackeados, o que acabou com a privacidade que muitas pessoas acreditavam ter.

Dessa forma, a criação de ataques contra a privacidade em redes se torna um assunto cada vez mais interessante por dois motivos principais: é mais fácil se proteger de ataques que são conhecidos, de modo que empresas criem os ataques para testar os níveis de proteção contra os mesmos; informações importantes podem ser extraídas dessas redes, como a confirmação de troca de mensagens entre dois usuários distintos.

1.3 Objetivo

O objetivo deste trabalho é apresentar um algoritmo desenvolvido para identificar nós pré-determinados no caso das redes em que não se tem informação sobre as relações entre os demais nós, como a rede de e-mail citada. Isto é, nas redes trabalhadas, cada usuário conhece apenas as suas relações, sendo o objetivo do trabalho encontrar relações entre os nós atacados. Este algoritmo seguirá os princípios de um ataque ativo.

A identificação dos nós escolhidos para serem atacados será feita em grafos não-direcionados e anonimizados, a partir da estrutura da rede. O algoritmo foi elaborado com o intuito de não existir restrição quanto ao número de nós atacados, isto é, a ideia é tornar possível a identificação de qualquer quantidade de nós na rede, inclusive de todos os nós. Para isso, também é levado em consideração que o número de nós a serem adicionados na rede, por ser um ataque ativo, deverá ser um número pequeno quando comparado ao tamanho da rede. O cálculo de número de nós a serem adicionados, chamados de nós atacantes, será detalhado no capítulo 3.

Além disso, a eficácia do método será analisada, para diferentes conjuntos de nós atacados, de tamanhos distintos. Serão considerados apenas dois possíveis resultados

do algoritmo: sucesso, quando todos os nós atacados foram identificados, e falha. Para isso, diferentes redes serão analisadas no capítulo 4, como o modelo Erdõs-Rényi e redes reais, fazendo um estudo comparativo em relação ao número de nós atacados. De modo a tornar possível a avaliação do método, isto é, averiguar quantas vezes foi sucedido ou não, este trabalho irá analisar redes não anonimizadas, simulando a anonimização após a criação dos atacantes.

A escolha pelo ataque ativo ocorreu de modo a tornar possível o ataque a qualquer rede, sem a necessidade do atacante já estar infiltrado na mesma. Este trabalho não irá abordar a probabilidade deste ataque ser detectado, que é a maior desvantagem deste tipo de ataque, segundo [2]. Os grafos não-direcionados, por sua vez, foram optados devido a maior dificuldade em trabalhar com estes na identificação de nós, entretanto, o algoritmo pode ser facilmente alterado de modo a aceitar grafos direcionados.

1.4 A técnica

A técnica desenvolvida terá duas componentes principais: a criação de nós atacantes e a identificação dos nós atacados, que será feita pela recuperação do subgrafo criado no ataque, isto é, subgrafo composto pelos nós atacantes.

A partir de um grafo não-direcionado e um conjunto de nós a serem atacados, serão criados $\mathcal{O}(\log n)$ novos nós, isto é, nós atacantes. Cada atacante terá um identificador, que será $atacante_x$, sendo $0 \leq x \leq (atacantes - 1)$.

A criação das arestas entre os nós atacantes será feita da seguinte forma: todo par (x_i,x_{i+1}) terá uma aresta, incluindo o par entre o atacante 0 e o último atacante, de modo a fechar um círculo entre os atacantes. Todas as demais arestas (x_i,x_j) são incluídas independentemente com probabilidade 1/2.

Em seguida, as arestas entre os nós atacantes e os nós atacados serão adicionadas. Cada nó atacado irá se conectar a um subconjunto de nós atacantes, e cada subconjunto destes precisa ser diferente dos demais, uma vez que se o processo de recuperação for capaz de identificar todos os nós atacantes, a identidade de todos os nós atacados será revelada.

Por fim, é calculado um grau máximo para cada atacante, maior ou igual ao grau que ele já possui até o momento. Cada atacante irá se conectar a nós não atacados, até atingir seu grau máximo ou até não terem mais nós a se conectar: quando todos os nós do grafo são atacados, não existem nós não atacados para completar o grau dos atacantes.

Para a recuperação do subgrafo criado, o atacante possui apenas a informação relativa aos nós e arestas que ele criou, uma vez que nas redes estudadas a informação estrutural da rede, como grau de cada nó, não é revelada. Este processo irá procurar,

a partir da estrutura da rede, os nós atacantes em ordem. Isto é, o primeiro passo do processo é procurar pelo atacante 0, o qual se sabe o grau e a sequência de grau dos vizinhos dele que também são atacantes. Dessa forma, o algoritmo irá fazer uma varredura no grafo em busca de nós com o grau igual ao grau deste atacante e com uma sequência de grau dos vizinhos que contenha a sequência de graus dos vizinhos atacantes. Este processo é repetido para todos os nós atacantes, até identificar todos ou chegar à conclusão que não é possível fazer a identificação, resultando em falha.

A partir da maneira como os nós atacados foram relacionados aos nós atacantes, se for possível identificar todos os nós atacante na rede anonimizada, então será possível identificar todos os nós atacados. Como cada nó atacado está conectado ao a um subconjunto de nós atacantes diferentes e todos os nós atacantes foram identificados na rede, é possível a partir dessas informações identificar os nós atacados.

O algoritmo completo é apresentado detalhadamente no capítulo 3.

1.5 Estruturação do documento

No capítulo 2, veremos alguns trabalhos relacionados, isto é, outros trabalhos que fizeram uso do aspecto estrutural de redes anonimizadas para a identificação de determinados nós. O capítulo 3 detalhe o algoritmo proposto, bem como a tecnologia envolvida no desenvolvimento do mesmo. O capítulo 4 apresenta os resultados de diferentes execuções do método apresentado. Por fim, o capítulo 5 apresenta conclusões a respeito do método e possíveis extensões e melhorias em trabalhos futuros.

Capítulo 2

Trabalhos Relacionados

Capítulo 3

Algoritmo proposto

3.1 Explicação detalhada

A explicação em alto nível já foi feita no capítulo de introdução. Em cada subseção a seguir, um componente específico será explicado detalhadamente.

3.1.1 Criação dos atacantes

Este processo recebe como entrada o grafo a ser atacado e os nós específicos a serem atacados. O número de nós atacados pode variar entre um e todos os nós do grafo.

3.1.2 Anonimização do grafo

A proposta deste trabalho é identificar nós pré-determinados, também chamados de nós atacados, de modo a revelar relações entre eles. Para ser possível analisar a eficiência do algoritmo proposto, isto é, se o mesmo é capaz de identificar os nós atacados ou não, é necessário conhecer a identificação de cada nó na rede, de modo que seja possível comparar o resultado encontrado para cada nó com a informação original.

Na ideia original, inicialmente o atacante só conhece todos os nós da rede, adicionando, em seguida, os novos usuários. Em seguida, os detentores da rede anonimizam seus nós, isto é, removem a informação crucial que identificava cada nó, e divulgam a rede assim. Este componente fará exatamente isso, isto é, ele simulará a anonimização da rede a ser divulgada.

Esse processo recebe como entrada a rede gerada pelo processo anterior, isto é, a rede inicial com os nós atacantes adicionados e todas as arestas entre eles e os nós da rede inicial. A saída dele, por sua vez, são dois arquivos: a rede anonimizada, isto é, a mesma rede de entrada, porém com os identificadores anonimizados que foram gerados; o mapeamento de cada nó, ou seja, um mapa entre a identificação

que cada nó possuía na rede de entrada e o novo id anônimo gerado. Este arquivo será utilizado para analisar a eficiência do método no final, ao tentar identificar os nós atacados, comparando cada resultado encontrado com o resultado oficial.

- Para a geração dos identificadores, todos os identificadores reais de cada nó são dispostos em uma lista e existem duas opções para gerar a troca de identidade:

    1. Cada nó recebe identificador aleatório, que será o índice do seu identificador real na lista com todos os identificadores
    2. Cada nó recebe o identificador de outro nó, isto é, ocorre a permutação entre os identificadores existentes.

    Para exemplificar, a figura 3.1 representa um grafo com 5 nós e arestas não-direcionadas entre eles.

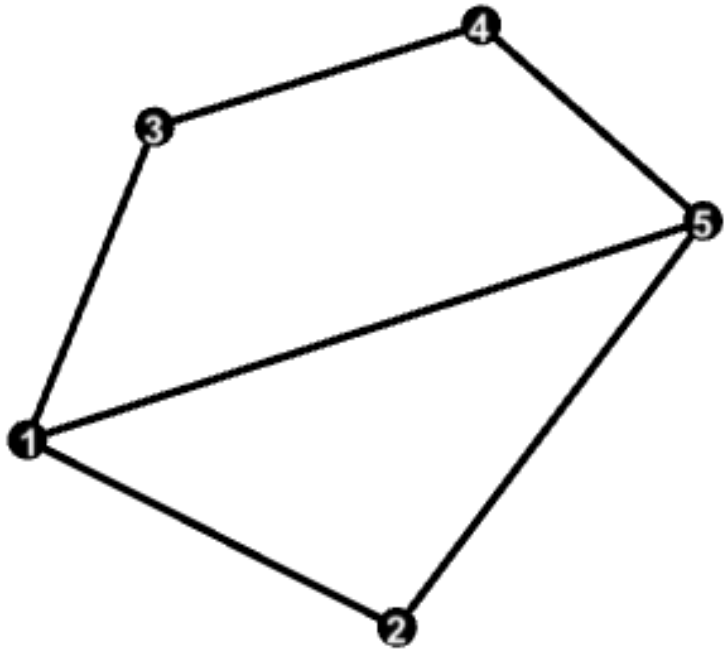

Figura 3.1: Grafo para exemplificar componente de anonimização.

Como este processo é aleatório, diferentes execuções com os mesmos parâmetros podem gerar arquivos de saída diferentes. A fim de exemplificação, as tabelas abaixo representam possíveis resultados extraídos do algoritmo de acordo com a geração dos identificadores:

Tabela 3.1: Tabela representando resultados do processo de anonimização a partir do índice de cada nó

Identificador Real	**Identificador Anonimizado**
2	4
3	2
4	0
1	3
5	1

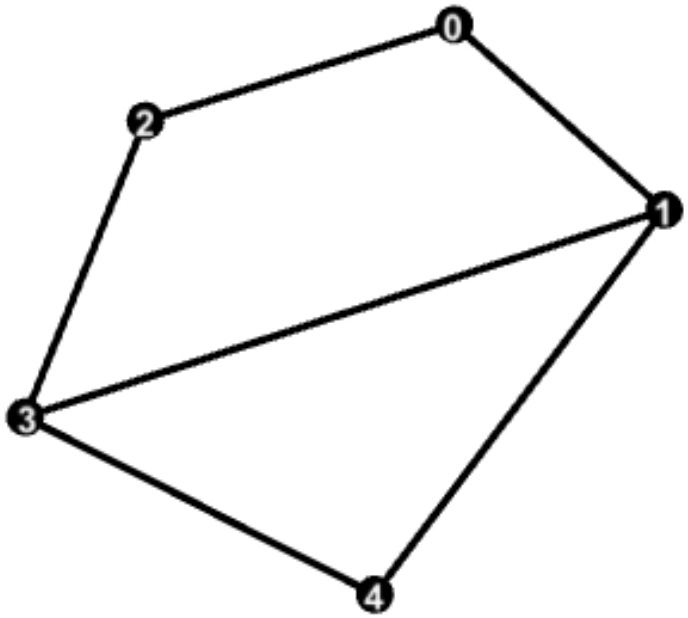

Figura 3.2: Grafo anonimizado pelo processo de anonimização a partir do índice de cada nó.

Tabela 3.2: Tabela representando resultados do processo de anonimização a partir da permutação entre os identificadores

Identificador Real	**Identificador Anonimizado**
4	5
3	3
2	4
1	2
5	1

Tabela 3.2 – continuação

Identificador Real	Identificador Anonimizado

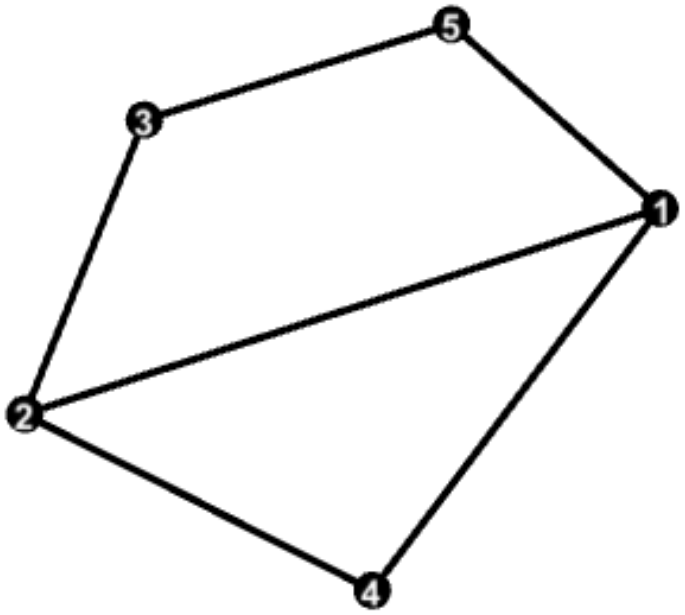

Figura 3.3: Grafo anonimizado pelo processo de anonimização a partir da permutação entre os identificadores.

3.1.3 Recuperação do subgrafo

Capítulo 4

Avaliação

Capítulo 5

Detecção de Comunidade

Capítulo 6

Conclusão e Trabalhos Futuros

6.1 Conclusão

6.2 Trabalhos Futuros

Referências Bibliográficas

[1] WIKIPEDIA - THE FREE ENCYCLOPEDIA. “Netflix Prize”. . https://en.wikipedia.org/wiki/Netflix_Prize, jul. 2017. Acessado em julho de 2017.

[2] BACKSTROM, LARS; KLEINBERG, JON; DWORK, CYNTHIA;. “Wherefore Art Thou R3579X? Anonymized Social Networks, Hidden Patterns, and Structural Steganography”. . https://utd.edu/~mxk055100/courses/privacy08f_files/social-network-privacy-backstrom.pdf, mai. 2007. Acessado em julho de 2017.