PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Programa de Pós-Graduação em Informática

Hélder Seixas Lima

FRAMEWORKS PARA VALIDAÇÃO DE ATRIBUTOS DE PERFIL DE USUÁRIOS DE REDE SOCIAL *ON-LINE*

Belo Horizonte

2018

Hélder Seixas Lima

FRAMEWORKS PARA VALIDAÇÃO DE ATRIBUTOS DE PERFIL DE USUÁRIOS DE REDE SOCIAL *ON-LINE*

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica de Minas Gerais, como requisito parcial para obtenção do título de Mestre em Informática.

Orientador: Prof. Humberto Torres Marques Neto

Belo Horizonte

2018

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

Lima, Helder Seixas
L732f *Frameworks* para validação de atributos de perfil de usuários de rede social *on-line* / Helder Seixas Lima. Belo Horizonte, 2018.
64 f. : il.

Orientador: Humberto Torres Marques Neto
Dissertação (Mestrado) – Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Informática

1. Redes sociais on-line - Análise. 2. Internet (Redes de computação). 3. Mensagens instantâneas. 4. Software - Desenvolvimento. 5. Usuários da Internet - Comportamento. I. Marques Neto, Humberto Torres. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Informática. III. Título.

CDU: 681.3.01:621.39

Ficha catalográfica elaborada por Fernanda Paim Brito - CRB 6/2999

Hélder Seixas Lima

FRAMEWORKS PARA VALIDAÇÃO DE ATRIBUTOS DE PERFIL DE USUÁRIOS DE REDE SOCIAL *ON-LINE*

Dissertação apresentada ao Programa de Pós-Graduação em Informática como requisito parcial para qualificação ao Grau de Mestre em Informática pela Pontifícia Universidade Católica de Minas Gerais.

Prof. Humberto Torres Marques Neto
PUC Minas

Prof. Mark Alan Junho Song
PUC Minas

Prof. Artur Ziviani
Laboratório Nacional de Computação Científica

Belo Horizonte, 28 de setembro de 2018.

Ao meu filho Samuel

AGRADECIMENTOS

Agradeço a Deus pela graça de superar todas as barreiras para realização deste trabalho.

À minha esposa Kelly por compreender minhas ausências durante esses últimos anos e por todo seu companheirismo. Amo-te!

Aos meus pais, Maria e Afonso, por todo incentivo e amor recebido de vocês.

Aos meus irmãos Gláucio, Afonso Filho e Graziela, amigos, familiares e colegas de trabalho que, com certeza, torceram muito para que eu concluísse este mestrado.

Aos colegas do laboratório *Human Behavior and Software Engineering* (HUB-SE) que proporcionaram momentos de rico aprendizado, troca de experiências e também muita descontração (fundamental para tornar o ambiente de pesquisa mais leve).

Aos professores e demais funcionários do Programa de Pós-Graduação em Informática da PUC Minas, em especial ao meu orientador Prof. Humberto por me guiar nesta caminhada.

Ao Instituto Federal de Educação, Ciência e Tecnologia do Norte de Minas Gerais (IFNMG), onde trabalho, por ter me permitido dedicar à minha capacitação.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes) por sua política de apoio à capacitação que me permitiu realizar este trabalho.

"A beleza de ser um eterno aprendiz"

Gonzaguinha

RESUMO

Os usuários de uma rede social *on-line* são identificados por meio dos seus perfis, os quais geralmente são compostos por atributos como nome, sexo, idade, cidade, entre outros. Como os atributos de perfil são autodeclarados, surge a possibilidade de que usuários mal-intencionados criem contas com informações falsas. Este trabalho tem como objetivo propor e analisar experimentalmente *frameworks* que determinem níveis de confiabilidade para os atributos de perfil de usuários de rede social *on-line*. Sendo que dois *frameworks* foram propostos: (i) *EgoNetwork-Checker*, que utiliza abordagem baseada em grafo e (ii) *MyFriends-Checker*, que utiliza abordagem baseada em votação apoiada por *crowdsourcing*. Ambos *frameworks* foram experimentalmente avaliados comparando amostras de atributos de perfil reais com amostras de atributos de perfil falsos. Em ambos os casos, a maioria dos atributos de perfil reais obtiveram níveis de confiabilidade maiores que os atributos de perfil falsos. Os resultados obtidos indicam que as premissas e abordagens consideradas na formulação desses *frameworks* contribuem para determinar níveis de confiabilidade dos atributos de perfil de usuários de rede social *on-line*.

Palavras-chave: rede social *on-line*, validação de identidade, validação de atributos de perfil.

ABSTRACT

Online social network users identify themselves through their profiles, which are usually composed of attributes such as name, gender, age, city, among others. Because profile attributes are self-declared, the possibility arises that malicious users create accounts with false information. This work proposes and analyzes experimentally frameworks that determine trustworthiness levels for the profile attributes of online social network users. We proposed two frameworks: (i) EgoNetwork-Checker that uses a graph-based approach and (ii) MyFriends-Checker that uses a crowdsourcing-based voting approach. Both frameworks were experimentally evaluated comparing samples of real profile attributes with samples of false profile attributes. In both cases, most of the real profile attributes have obtained higher trustworthiness levels than the false profile attributes. The results indicate that the assumptions and approaches considered in the formulation of these frameworks contribute to determining trustworthiness levels of the profile attributes of online social network users.

Keywords: online social network, identity validation, profile attribute validation.

LISTA DE FIGURAS

FIGURA 1 – Exemplos de tipos de grafos 15

FIGURA 2 – Fechamento triádico 16

FIGURA 3 – Estrutura de uma rede de amizades 20

FIGURA 4 – Ilustração de uma *ego-network* 21

FIGURA 5 – Tipos de trabalhos e abordagens para identificar, combater e/ou validar usuários maliciosos de rede social *on-line* 23

FIGURA 6 – Metodologia adotada 27

FIGURA 7 – Primeiro módulo do *EgoNetwork-Checker* 30

FIGURA 8 – Segundo módulo do *EgoNetwork-Checker* 31

FIGURA 9 – Exemplo da validação de um atributo de perfil no *MyFriends-Checker* 33

FIGURA 10 – Distribuição de h_i nas amostras de dados considerando $n_{\mathrm{i}} \geqslant 3$ e $n_{\mathrm{i}} \geqslant 9$ 35

FIGURA 11 – Distribuição de h_i por tipo de atributo de perfil nas amostras de dados considerando $n_{\mathrm{i}} \geqslant 9$ 36

FIGURA 12 – Distribuição de g_i nas amostras de dados considerando $n_{\mathrm{i}} \geqslant 3$ e $n_{\mathrm{i}} \geqslant 9$ 36

FIGURA 13 – Distribuição de g_i por tipo de atributo de perfil nas amostras de dados considerando $n_{\mathrm{i}} \geqslant 9$ 37

FIGURA 14 – Distribuição de t_i nas amostras de dados 39

FIGURA 15 – Distribuição de t_i por tipo de atributo de perfil nas amostras de dados . . . 39

FIGURA 16 – Exemplos de perguntas do *MyFriends-Quiz* sobre atributos de perfil 41

FIGURA 17 – Exemplo de pergunta do *MyFriends-Quiz* sobre tipo de relacionamento entre usuários 42

FIGURA 18 – Rede de usuários do *MyFriends-Quiz* 43

FIGURA 19 – Avaliações dos atributos de perfil no *MyFriends-Quiz* 46

FIGURA 20 – Avaliações dos atributos de perfil no *MyFriends-Quiz* por tipo 47

FIGURA 21 – Avaliações dos tipos de relacionamento entre usuários do *MyFriends-Quiz* 49

FIGURA 22 – Avaliações dos tipos de relacionamento entre usuários do *MyFriends-Quiz* detalhado 50

FIGURA 23 – Distribuição da porcentagem de amigos ou amigos indiretos que conhecem pessoalmente os usuários das amostras 50

FIGURA 24 – Modelo da implementação experimental do *MyFriends-Checker* 51

FIGURA 25 – Níveis de confiabilidade dos atributos de perfil obtidos com o *MyFriends-Checker* 52

FIGURA 26 – Níveis de confiabilidade dos atributos de perfil obtidos com o *MyFriends-Checker* detalhados por tipo 53

FIGURA 27 – Correlação dos níveis de confiabilidade dos atributos de perfil obtidos com o *MyFriends-Checker* e a soma dos pesos dos avaliadores 53

FIGURA 28 – Questionário aplicado aos usuários do *MyFriends-Quiz* 64

LISTA DE TABELAS

TABELA 1 – Resultados do *Módulo 1* do *EgoNetwork-Checker* para os atributos de perfil do tipo cidade, empresa, escola e profissão 38

TABELA 2 – Quantidade e porcentagem de usuários do *MyFriends-Quiz* que possuem atributos de perfil 43

TABELA 3 – Atributos de perfil mais comuns entre os usuários do *MyFriends-Quiz* por tipo 45

LISTA DE ABREVIATURAS E SIGLAS

CDF – Função de Distribuição Cumulativa

CCDF – Função de Distribuição Cumulativa Complementar

API – *Application Programming Interface*

SUMÁRIO

1 INTRODUÇÃO **9**

1.1 Problema 10

1.2 Objetivo 11

1.2.1 Objetivos específicos 11

1.3 Justificativa 11

1.4 Estrutura do texto 13

2 REFERENCIAL TEÓRICO **14**

2.1 Teoria das redes complexas 14

2.1.1 Conceitos e métricas de redes complexas 14

2.2 Redes sociais *on-line* 16

2.2.1 Tipos de usuários maliciosos 17

2.2.2 Análise de redes sociais 18

2.2.2.1 Fenômeno da homofilia 18

2.2.2.2 Fenômeno do mundo pequeno e fechamento triádico 19

2.2.2.3 *Ego-network* 20

2.3 *Crowdsourcing* 21

2.4 Gamificação 21

3 TRABALHOS RELACIONADOS **23**

4 *FRAMEWORKS* PROPOSTOS **27**

4.1 *Framework EgoNetwork-Checker* 27

4.1.1 Premissas 28

4.1.2 Métricas de ego-network 28

4.1.3 Definição do framework 29

4.1.3.1 Módulo 1: Preparação 29

4.1.3.2 Módulo 2: Cálculo do nível de confiabilidade de atributos de perfil 30

4.2 *Framework MyFriends-Checker* 31

4.2.1 Premissas 32
4.2.2 Definição do framework 32

5 ANÁLISE EXPERIMENTAL DOS *FRAMEWORKS* **34**
5.1 *Framework EgoNetwork-Checker* 34
5.1.1 Definição das amostras de dados 34
5.1.2 Características das amostras de dados 35
5.1.3 Implementação do framework e análise dos resultados 36
5.1.4 Análise da complexidade 39
5.2 *Framework MyFriends-Checker* 40
5.2.1 MyFriends-Quiz 40
5.2.2 Usuários do MyFriends-Quiz 42
5.2.2.1 Características da rede 42
5.2.2.2 Características dos nós 43
5.2.3 Ground truth 44
5.2.3.1 Atributos de perfil 44
5.2.3.2 Tipo de relacionamento 48
5.2.4 Implementação do framework e análise dos resultados 51
5.2.5 Análise da complexidade 54
5.2.6 Comparação com o FaceTrust 54

6 CONCLUSÕES **56**

REFERÊNCIAS **58**

APÊNDICE A -- QUESTIONÁRIO *MYFRIENDS-QUIZ* **64**

1 INTRODUÇÃO

As redes sociais *on-line* fornecem um ambiente virtual para comunicação e interação entre seus usuários. Aproximadamente dois bilhões de pessoas participam dessas redes em todo o mundo[1], tornando este serviço um dos mais populares da *web*. Um usuário de uma rede social *on-line* é identificado por meio de um perfil autodeclarado que geralmente consiste em uma foto e informações pessoais como nome, idade, sexo, cidade, escola, profissão, empresa entre outros dados. O nível de detalhe dos perfis de usuário varia de acordo com a rede social, enquanto o Facebook, o Google+ e o LinkedIn permitem o registro de perfis detalhados, o Twitter e o Instagram permitem dados reduzidos para descrever um perfil.

A falsificação de perfil em redes sociais *on-line* é possível porque os perfis de usuários são autodeclarados e os *sites* de redes sociais não exigem a comprovação dos dados informados. Existem três tipos de perfis maliciosos: perfis falsos (pessoas que não existem no mundo real), perfis clonados (uma pessoa que finge ser outra pessoa que existe no mundo real) e perfis comprometidos (uma pessoa com intenção maliciosa que invade o perfil de outro usuário) (SOLIMAN et al., 2016). É muito comum esses três tipos de perfis serem operados por meio de robôs, popularmente chamados de *bots*, que são programados para executar ações predefinidas nas redes socias. Algumas redes, tais como Facebook e Google+, implementaram procedimentos para que sejam mais confiáveis, como a confirmação do número de telefone e/ou *e-mail*. Outro recurso aplicado em redes sociais *on-line* é permitir que seus usuários relatem contas suspeitas. No entanto, embora existam tais iniciativas, a validação da identidade de usuários em tais redes continua sendo um problema em aberto (RAMALINGAM; CHINNAIAH, 2018).

Tradicionalmente esses perfis maliciosos são responsáveis pela propagação de *spams* e *malwares* nas redes sociais *on-line* (GAO et al., 2010). Mais recentemente perfis maliciosos estão sendo utilizados para impulsionar notícias falsas nessas redes e em algumas situações chegaram a influenciar eleições[2]. O rol de práticas indesejáveis praticadas por perfis maliciosos é vasto; vão desde namorado falso na *Internet*[3], passando por crimes de estelionato[4] e até casos de pedofilia[5].

[1] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users

[2] https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

[3] http://g1.globo.com/fantastico/noticia/2015/08/homem-aciona-policia-ao-se-apaixonar-por-perfil-falso-em-rede-social.html

[4] https://g1.globo.com/ma/maranhao/noticia/perfis-falsos-em-redes-sociais-sao-usados-para-aplicar-golpes-no-ma.ghtml

[5] https://g1.globo.com/sao-paulo/sao-jose-do-rio-preto-aracatuba/noticia/suspeita-de-criar-fake-para-aliciar-criancas-tem-computador-apreendido-em-operacao.ghtml

O pressuposto de que as identidades em uma rede social *on-line* são verdadeiras é condição fundamental para tornar esses ambientes digitais mais confiáveis, pois, é por meio do seu perfil que um usuário será reconhecido pelos seus amigos e possibilitará a criação de novos contatos. A importância de verificar a validade das identidades não se restringe apenas ao aumento da confiabilidade interna da rede social; deve-se considerar o surgimento e popularização dos protocolos de autorização e autenticação que permite que um usuário de rede social acesse um sistema terceiro utilizando a identidade previamente declarada.

Neste trabalho foi realizada revisão da literatura a fim de identificar abordagens e *frameworks* dedicados ao combate de perfis maliciosos nas redes sociais. Dentre as abordagens estudadas duas foram consideradas pertinentes para a validação de atributos de perfil de usuários de rede social *on-line*: (i) abordagem baseada em grafo e (ii) abordagem baseada em votação.

Desta forma, este trabalho tem como contribuição a proposta de dois *frameworks* para validação de atributos de perfil de usuários de rede social *on-line*. O primeiro chama-se *EgoNetwork-Checker* que utiliza abordagem baseada em grafo e visa determinar níveis de confiabilidade para os atributos de perfil por meio da verificação da coerência da *ego-network* do usuário com fenômenos comuns nas redes sociais. O outro *framework* proposto neste trabalho é referenciado por *MyFriends-Checker* que utiliza abordagem baseada em votação apoiada por *crowdsourcing* para atribuir níveis de confiabilidade aos atributos de perfil de usuários de rede social *on-line*. Este trabalho considerou duas abordagens distintas para resolver o mesmo problema com o intuito de analisar experimentalmente os resultados de cada uma das abordagens consideradas.

Ambos *frameworks* foram experimentalmente avaliados comparando amostras de atributos de perfil reais com amostras de atributos de perfil falsos. Em ambos os casos a maioria dos atributos de perfil reais obtiveram níveis de confiabilidade maiores que os atributos de perfil falsos. Os resultados obtidos indicam que as premissas e abordagens consideradas na formulação desses *frameworks* contribuem para determinar níveis de confiabilidade dos atributos de perfil de usuários de rede social *on-line*.

1.1 Problema

O problema de pesquisa deste trabalho é sintetizado na seguinte pergunta:

- Como validar a veracidade de atributos de perfil autodeclarados por usuários de rede social *on-line*?

1.2 Objetivo

O objetivo geral deste trabalho é propor e analisar experimentalmente *frameworks* que determinem níveis de confiabilidade para os atributos de perfil de usuários de rede social *on-line*.

1.2.1 Objetivos específicos

- Propor e analisar experimentalmente *framework* que determine níveis de confiabilidade para os atributos de perfil de usuários de rede social *on-line* utilizando abordagem baseada em grafo.
- Propor e analisar experimentalmente *framework* que determine níveis de confiabilidade para os atributos de perfil de usuários de rede social *on-line* utilizando abordagem baseada em votação apoiada por *crowdsourcing*.

1.3 Justificativa

A primeira justificativa para este trabalho é contribuir para aumentar a confiança e segurança de usuários de redes sociais *on-line*, sendo proposto verificar o nível de confiabilidade dos atributos de perfil de qualquer um desses usuários. Contudo, uma reflexão mais ampla é necessária para se compreender todas as possibilidades que surgem com a validação da identidade de usuários dessas redes.

A *Internet* tem modificado várias atividades do cotidiano da sociedade. Se a popularização das redes sociais *on-line* representou uma transformação da forma como as pessoas se socializam, o surgimento de serviços da chamada economia de compartilhamento também tem representado uma grande mudança na maneira como se fazem negócios e se prestam serviços nos dias atuais. Aplicativos de transporte como o Uber[6] e soluções de hospedagem como o Airbnb[7], são os grandes expoentes dessa nova economia que se caracteriza por utilizar a tecnologia para aperfeiçoar serviços numa perspectiva *peer-to-peer*. Com isso, as relações deixam de ser entre pessoa-empresa e passam a ser entre pessoa-pessoa (HAMARI; SJÖKLINT; UKKONEN, 2015).

Nesse tipo de economia é fundamental que os usuários tenham confiança mútua, tanto quem irá prestar um serviço como quem irá consumir. Os envolvidos nessas relações da economia de compartilhamento devem apresentar uma identidade no 'mundo digital' correspondente a uma pessoa real na sociedade para que as condições mínimas de confiança sejam estabelecidas (HAWLITSCHEK; TEUBNER; WEINHARDT, 2016).

[6] https://www.uber.com/
[7] https://www.airbnb.com/

A evolução da *Internet* também tem contribuído para o desenvolvimento de novas perspectivas em questões relacionadas à gestão pública; iniciativas nessa área buscam ampliar o significado de participação popular e democracia por meio da adoção de mecanismos proporcionados pelo avanço tecnológico. O termo *e-democracy*, combinação das palavras inglesas *eletronic* e *democracy*, refere-se ao uso de meios eletrônicos e de comunicação para empoderamento do cidadão na fiscalização e participação de questões de domínio público a fim de culminar na efetiva participação da sociedade nos processos de tomada de decisão (PELAEZ et al., 2016). Hoje já existem iniciativas independentes de participação social na *Internet* como o *site* de petições *online* Avaaz[8], e o Mudamos[9], aplicativo de assinatura de projetos de leis de iniciativa popular. Também existem iniciativas na esfera pública como o sistema e-Cidadania[10] do Senado Federal, onde se promovem consultas públicas permitindo à população se manifestar a favor ou contra projetos de lei que estão tramitando no Congresso Nacional. Em todos esses sistemas da *e-democracy* foi constatado que o cadastro é feito informando apenas alguns dados pessoais e que não há nenhum processo para validação da identidade do usuário.

À medida que a *Internet* se integra cada vez mais nas relações sociais e comerciais, aumenta a demanda para validação de identidades *on-line*. Nesse sentido, algumas iniciativas já são aplicadas por setores da economia, sendo possível citar como exemplo o atendimento bancário na *Internet*, em que se desenvolveram processos robustos para certificar maior segurança nas operações remotas. No Brasil, a Receita Federal já oferece serviço de emissão de certificado digital para pessoa física, chamado de e-CPF[11], sendo utilizado em alguns procedimentos disponibilizados na *Internet* por esse órgão. O e-CPF garante a autenticidade da pessoa física e a integridade das informações transmitidas pela rede, sendo aplicado aos sistemas que exigem um alto grau de segurança. Para emitir esse certificado é necessário deslocar-se até uma certificadora reconhecida pela Receita Federal, apresentar documentação exigida e arcar com uma despesa mínima de R$ 90,00 ao ano.

Vários sistemas de participação coletiva na *Internet* e serviços da economia de compartilhamento podem ter como requisito que os seus usuários sejam de fato pessoas reais existentes na sociedade e que os atributos de perfil que estejam declarando sejam verdadeiros. Porém, condicionar o acesso do usuário à posse de um certificado digital como o e-CPF ou desenvolver processos de validação como do setor bancário, pode inviabilizar sua utilização para boa parte do público alvo por conta da burocracia e dos custos envolvidos.

Desta forma, este trabalho se justifica por contribuir para a validação de identidade *on-line* que coopera para proporcionar um ambiente mais seguro e confiável aos usuários da *Internet*, tanto dentro das redes sociais como em outros serviços que estabeleçam a criação de relações entre as pessoas.

[8] http://avaaz.org
[9] https://www.mudamos.org/
[10] https://www12.senado.leg.br/ecidadania/
[11] http://idg.receita.fazenda.gov.br/orientacao/tributaria/senhas-e-procuracoes/senhas/certificados-digitais

1.4 Estrutura do texto

Este trabalho está organizado da seguinte maneira: no Capítulo 2 é apresentado o referencial teórico que fundamenta esta pesquisa. O Capítulo 3 contém revisão da literatura sobre trabalhos que visam identificar, combater e validar usuários maliciosos de rede social *on-line*. No Capítulo 4 são descritas as metodologias dos dois *frameworks* propostos neste trabalho: *EgoNetwork-Checker* e *MyFriends-Checker*. No Capítulo 5 análises experimentais dos frameworks propostos são apresentadas. Por fim, no Capítulo 6 encontra-se as conclusões e os trabalhos futuros.

2 REFERENCIAL TEÓRICO

Neste capítulo são apresentados conceitos fundamentais para compreensão deste trabalho. A Seção 2.1 apresenta a teoria das redes complexas que fornece métricas que ajudam a caracterizar e compreender fenômenos presentes nas redes sociais *on-line* que são apresentados na Seção 2.2. Na Seção 2.3 e na Seção 2.4 são apresentados os conceitos de *crowdsourcing* e gamificação, respectivamente, áreas de estudos que foram exploradas no contexto do *framework MyFriends-Checker*.

2.1 Teoria das redes complexas

A teoria das redes complexas é uma área de conhecimento multidisciplinar que visa caracterizar, estudar e resolver problemas conhecidos do mundo real por meio da representação desses eventos na forma de redes e das implicações no entorno da sua formação, comportamento e evolução (EASLEY; KLEINBERG, 2010; NEWMAN, 2003b). Uma rede é qualquer estrutura em que existam ligações entre objetos que a compõem, podendo ser citados como exemplo as redes de telefônica móvel, uma malha rodoviária, as rotas de entrega de uma empresa de logística, redes de aeroportos, as redes urbanas de energia e esgoto, *Internet*, redes sociais, redes neurais do cérebro, cadeia de proteínas e outras (EASLEY; KLEINBERG, 2010; NEWMAN, 2003b).

A associação da teoria dos grafos com a teoria das redes complexas contribui para compreensão de problemas. Com isso, uma série de métricas foi criada com o objetivo de identificar e dimensionar fenômenos recorrentes nas redes. No tópico a seguir são apresentados alguns conceitos e métricas de redes complexas importantes para estes trabalho.

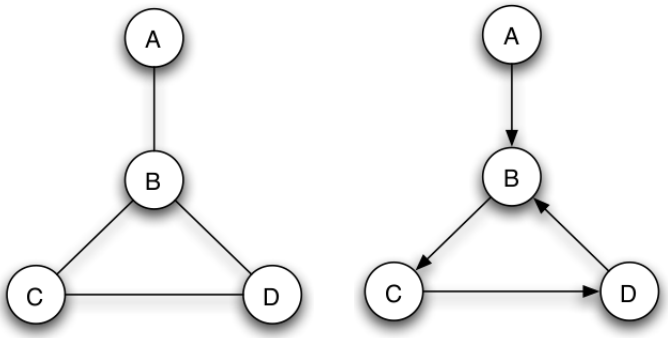
2.1.1 Conceitos e métricas de redes complexas

As métricas e conceitos a seguir são fundamentais para análise de redes a partir da teoria dos grafos. Eles foram extraídos de Easley e Kleinberg (2010) e Newman (2003b).

Uma rede ou grafo consiste em um conjunto de nós (vértices) e suas conexões (arestas). Com isso, são chamados de *vizinhos* dois nós em que há uma aresta ligando-os diretamente. Diz-se haver *conectividade* quando há existência de algum *caminho* que possa ligar dois nós, ou seja, existe alguma forma de ir de um nó de origem até um nó de destino passando por arestas. Os grafos são classificados como direcionado ou não direcionado, sendo que o primeiro também é conhecido como dígrafo e o segundo normalmente é referenciado simplesmente como grafo. No caso dos grafos não direcionados, toda aresta entre dois vizinhos pressupõe a existência de

conectividade entre eles, enquanto que no caso dos dígrafos isso depende da direção da aresta que estabelece um nó de origem e um nó de destino. A Figura 1 ilustra os dois tipos de grafos.

Figura 1 – Exemplos de tipos de grafos
(a)Grafo com 4 nós (b)Dígrafo com 4 nós



Fonte: Adaptado de Easley e Kleinberg (2010)

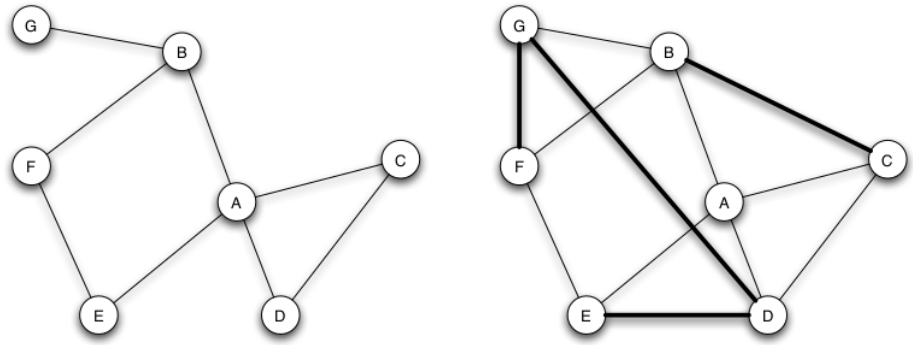
Um grafo será um *componente* único quando houver *conectividade* entre todos os seus nós, ou seja, há um caminho entre todos os nós da rede. Haverá mais ocorrências de *componentes* em um grafo quando houver nós sem *conectividade* com outros; com isso, compreende-se *componente* como um conjunto de vértices onde há *conectividade* entre todos eles. O número de arestas que há entre dois nós de um componente é denominado de *distância*, e *componente gigante* é o nome dado ao *componente* do grafo que possui maior número de nós.

O termo *grau* se refere ao número de arestas conectadas a um nó. Em grafos direcionados haverá *grau de entrada* e de *grau de saída*. Essa medida é muito importante para se identificar os nós que possuam maior centralidade numa rede.

Muitas redes caracterizam-se por não serem estáticas, a observação do seu dinamismo é alvo de muitos estudos que visam compreender a predição de formação de arestas. O termo *fechamento triádico* é usado para referir ao princípio da formação de um triângulo entre três vértices. A Figura 2 ilustra casos de *fechamento triádico*, por exemplo; em um primeiro momento (a) é percebido o potencial para formação de um triângulo envolvendo os nós A, B e C, pois já havia arestas entre os nós A e B; e também entre A e C. No segundo momento (b) uma nova aresta entre B e C é criada e com isso se configurou formação de *fechamento triádico*. Na figura em questão também é ilustrada a criação de 2 *fechamentos triádicos* envolvendo os nós A-D-E e B-F-G.

Coeficiente de clustering, ou coeficiente de agrupamento, é uma medida utilizada para verificar o grau de aglomeração dos nós em uma rede. O cálculo do *coeficiente de clustering* de um nó corresponde à razão entre o número de arestas e o número de arestas possíveis entre seus vizinhos. As fórmulas para calcular o coeficiente de *clustering* de um nó em um grafo e um dígrafo são apresentadas respectivamente nas Equações 2.1 e 2.2, sendo k o conjunto de vizinhos do nó i e e o conjunto de arestas entre os nós de k. O *coeficiente de clustering* está estritamente vinculado ao conceito de *fechamento triádico*, pois, quanto maior o número de *fechamentos triádicos*, maior será o resultado do *coeficiente de clustering*.

Figura 2 – Fechamento triádico
(a)Antes das novas arestas (b)Depois das novas arestas



Fonte: Adaptado de Easley e Kleinberg (2010)

$$C_{\mathrm{i}} = \frac{2|e|}{|k|(|k|-1)} \tag{2.1}$$

$$C_{\mathrm{i}} = \frac{|e|}{|k|(|k|-1)} \tag{2.2}$$

2.2 Redes sociais *on-line*

Uma rede social *on-line* pode ser definida como um sistema que proporciona um ambiente na *Internet* para que usuários estabeleçam relação e comunicação com outros (BOYD; ELLISON, 2007). As redes sociais estão entre os tipos de serviços mais populares da *Internet*, sendo que em média os internautas americanos gastam 20% do seu tempo, enquanto navegam na rede mundial de computadores, acessando esse tipo de sistema[1]. São diversas redes sociais com diferentes propósitos, desde compartilhamento de fotos, vídeos, currículos e o mais comum que trata de relações de amizades, caso do Facebook e Google+.

Conforme dados de abril de 2018, aproximadamente dois bilhões de internautas participam de redes sociais *on-line* em todo o mundo[2]. A rede social Facebook é a mais popular atualmente, sendo a primeira a ter ultrapassado a marca de um bilhão de usuários ativos mensalmente. Outras redes sociais também se destacam por apresentarem características próprias e explorarem nichos específicos. Pode-se citar como exemplos o LinkedIn, rede social especializada no mercado de trabalho, o Twitter, que tem como caraterística peculiar permitir apenas a publicação de mensagens curtas, e o Instagram, que é uma rede social focada na publicação e compartilhamento de fotos.

[1] http://www.businessinsider.com/social-media-engagement-statistics-2013-12
[2] http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number- of-users

Apesar de haver redes sociais com focos diversos, em geral, as mais populares apresentam as mesmas características de compartilhamento de conteúdos multimídia. O que as diferenciam são algumas características relacionadas à privacidade e principalmente aos tipos de conexões com outros usuários da rede, por exemplo, considerando algumas das redes sociais mais populares no Brasil; no caso do Facebook e LinkedIn as conexões são sempre recíprocas, enquanto que no Twitter, Google+ e Instagram as conexões entre usuários não precisam ser recíprocas. Numa perspectiva de representação de redes complexas o Facebook e o LinkedIn consistem em grafos não direcionados, enquanto que o Twitter, Google+ e Instagram são representados como dígrafos. Neste trabalho, para fins de simplificação, a conexão entre dois usuários de uma rede social será referenciada como amizade, mesmo que a motivação da conexão seja por outro contexto social e o termo empregado pela rede social em questão seja outro.

Outra característica em que se nota diferença entre as redes é o nível de detalhamento do perfil do usuário, o Facebook, Google+ e LinkedIn se caracterizam por permitir o cadastramento de perfis com alto grau de detalhamento, contemplando desde os dados básicos até informações profissionais e acadêmicas, enquanto que o Twitter e Instagram prezam por perfis enxutos, contendo apenas os dados básicos.

2.2.1 Tipos de usuários maliciosos

Uma característica comum às redes sociais *on-line* mais populares é que os perfis dos usuários são autodeclarados e em geral não há processo para checagem se as informações são verdadeiras. Obviamente, essa metodologia adotada pelas redes sociais *on-line* visa tornar o processo de aquisição de usuários mais simples e ampliar o seu número de participantes. Entretanto, isso provoca a possibilidade da infiltração de perfis maliciosos que são criados com o intuito de ocultar a real identidade do seu operador. Geralmente os usuários maliciosos intencionam disseminar *spams*, divulgar notícias falsas, influenciar opiniões e promover ou denegrir pessoas, empresas e produtos (JIANG; CUI; FALOUTSOS, 2016). Soliman et al. (2016) identificaram três tipos de usuários maliciosos em redes sociais: perfis falsos, perfis clonados e contas comprometidas.

Os perfis falsos consistem em pessoas que não existem no mundo real. Pode ser alguma conta criada ingenuamente para um animal de estimação de uma pessoa[3] ou pode ter sido concebida para práticas mal intencionadas. Muitas vezes pode até ser operado por robôs, sendo empregado o termo *bot* social para se referir a esse tipo de usuário falso em redes sociais (DAVIS et al., 2016).

O termo *sybil* também é empregado para referenciar um perfil falso que é controlado por uma identidade oculta, ou até mesmo operado por robôs assim como os *bots* sociais. Esse tipo de conta falsa sustenta um tipo de fraude chamado de *sybil attack*, no qual vários *sybils* são criados por um indivíduo que intenciona legitimar a rede de usuários falsos criados e, com

[3]http://edition.cnn.com/2012/08/02/tech/social-media/facebook-fake-accounts/

isso, aplicar golpes em massa numa rede social. Esse tipo de ataque já recebe a atenção de pesquisadores há muito tempo, pois ele não se limita às redes sociais, sendo essa uma prática corriqueira em qualquer sistema do tipo *peer-to-peer* (DOUCEUR, 2002).

Por fim, os ataques de clonagem de perfil, que consiste em se passar por outra pessoa que realmente existe no mundo real, e os ataques de comprometimento de conta de usuário, em que uma pessoa mal-intencionada invade e toma o controle de uma conta de usuário, são práticas que juntamente com os ataques de perfis falsos tornam as redes sociais ambientes menos confiáveis, sendo necessário precaução com a privacidade pelos usuários e desenvolvimento de técnicas que mitiguem esses ataques por parte dos provedores de redes sociais *online*.

2.2.2 Análise de redes sociais

A análise de redes sociais é uma disciplina que estuda as estruturas sociais por intermédio da teoria das redes complexas (OTTE; ROUSSEAU, 2002). Nas subseções seguintes são apresentados os fenômenos da homofilia e do mundo pequeno, eventos importantes para compreender características da formação das redes sociais. Por fim, o conceito de *ego-network*, útil para compreensão deste trabalho, é apresentado.

2.2.2.1 Fenômeno da homofilia

"Diz-me com quem andas e te direi quem és". Esse provérbio exprime bem o conceito de homofilia, que se refere à tendência de as pessoas possuírem características semelhantes aos seus amigos (MCPHERSON; SMITH-LOVIN; COOK, 2001). O princípio da homofilia é algo já estudado pela sociologia; nesses estudos já se observou esse evento por características diversas como cor da pele, etnia, idade, gênero e também em características mutáveis como lugares onde se viveu, profissão, empresas em que se trabalhou, escolas frequentadas, classe social, interesses, crenças e opiniões (MCPHERSON; SMITH-LOVIN; COOK, 2001; CURRARINI; JACKSON; PIN, 2009; EASLEY; KLEINBERG, 2010).

O fenômeno da homofilia tem sido recorrentemente explorado por trabalhos que investigam as redes sociais *on-line*. Por exemplo, Bhattacharyya, Garg e Wu (2011) propuseram um modelo de detecção de similaridade entre os usuários do Facebook pela análise semântica dos atributos de perfil. Os resultados mostraram que o nível de similaridade é maior em pares de amigos do que em pares de pessoas aleatórias. Mukta, Ali e Mahmud (2016) desenvolveram um modelo de identificação e validação de tipos de personalidade de usuários de redes sociais com base em traços de homofilia. Kwak et al. (2010) verificaram a ocorrência de homofilia no Twitter considerando a localização geográfica e popularidade dos usuários. Outros trabalhos verificaram o fenômeno da homofilia nas redes sociais *on-line* considerando a preferência política dos usuários (HIMELBOIM et al., 2014; HALBERSTAM; KNIGHT, 2014; CAETANO et al., 2017).

Trabalhos de predição também consideraram o conceito de homofilia. Mislove et al. (2010) desenvolveram um método com taxa de precisão de 80% para inferir atributos ausentes em perfis de usuários usando indicadores de homofilia. Han et al. (2015) propuseram um método inspirado no princípio da homofilia para entender as preferências dos usuários sobre filmes, músicas, programas de televisão, entre outras. Eles concluíram que os níveis de homofilia em relação às preferências de um conjunto de usuários são maiores quando há semelhança nos atributos demográficos deles.

Newman (2003a) sugere uma fórmula para calcular o coeficiente de homofilia, também chamado de coeficiente de assortatividade, dos nós em uma rede considerando atributos discretos. Para quantificar o coeficiente de homofilia r se considera:

$$r = \frac{\sum_i e_{ii} - \sum_i a_i b_i}{1 - \sum_i a_i b_i}, \tag{2.3}$$

onde i corresponde a um valor de um atributo que caracteriza um nó da rede, e_{ii} é a fração de arestas que possuem nós com i nas suas duas extremidades e a_i e b_i são as frações de arestas que possuem um nó com valor de atributo i em alguma de suas extremidades. Em uma rede não direcionada $a_i = b_i$.

Assim, r admite valores entre -1 e 1, em que 1 representa uma rede em que todas as conexões são formadas entre nós que possuem i e -1 representa uma rede em que todas as arestas são formadas entre nós em que apenas um deles possui i. Há homofilia quando r é maior que zero.

2.2.2.2 Fenômeno do mundo pequeno e fechamento triádico

O fenômeno do mundo pequeno foi primeiramente descrito por Milgram (1967) que concluiu que uma pessoa está distante de outra em uma média de 6 graus de separação, ou seja, por meio de outras 6 pessoas é possível alcançar qualquer pessoa do mundo. Também demonstrou que as pessoas são capazes, de forma não coordenada, de realizar com sucesso uma busca a outra pessoa numa rede social. Para chegar a essa conclusão, foi realizado um experimento em que se enviaram 160 cartas a moradores de Boston e Omaha (Nebraska-EUA) que tinham a missão de repassar essas cartas aos seus conhecidos até chegar à pessoa alvo que era um morador de Sharon, Massachussets-EUA.

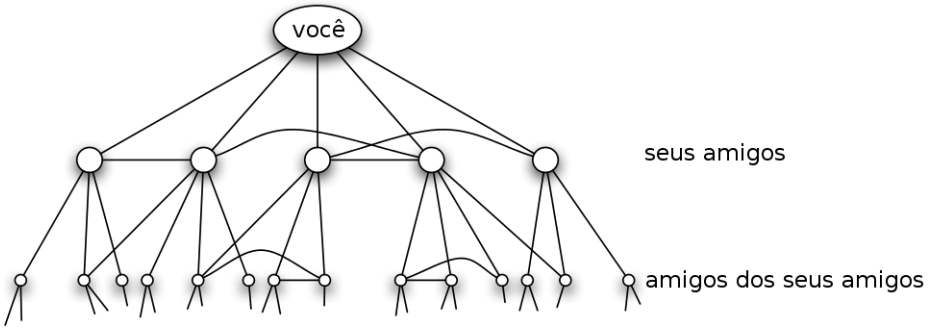
Em um primeiro momento, a afirmação de que todas as pessoas do mundo estão distantes em média a no máximo 6 intermediários parece ser inconsistente e isso coloca em suspeição os procedimentos metodológicos adotados em Milgram (1967), principalmente por ter sido considerada uma amostra pequena de pessoas e por estar restrito ao território de um único país. Porém, estudos maiores e já considerando os meios de comunicações digitais ratificaram o fenômeno do mundo pequeno. Este é o caso de Dodds, Muhamad e Watts (2003) que realizaram experimento semelhante, todavia, os autores enviaram *e-mails* para mais de

60 mil internautas visando alcançar 18 destinatários em 13 países diferentes. Foi encontrado que a distância entre a origem e o alvo varia de 5 a 7 pessoas em média.

Em Leskovec e Horvitz (2008), um estudo ainda mais amplo encontrou grande ocorrência de pequenos caminhos entre os usuários do *Microsoft Instant Mensenger*[4]. A base de dados em questão consistia de 240 milhões de pessoas espalhadas por todo o mundo, em que para o experimento foram selecionadas mil pessoas aleatoriamente e se calculou o menor caminho entre todas elas. O tamanho dos caminhos encontrados teve uma média de 6,6, tendo a mediana igual a 7 e a moda como 6. Caminhos muito longos são a exceção; houve um caso com 29 pessoas intermediárias, entretanto, 78% das pessoas puderam ser alcançadas em até 7 níveis de distância.

Os padrões observados de fechamento triádico, conceito apresentado na Seção 2.1.1, ajuda a compreender o fenômeno do mundo pequeno. A literatura mostra que o início de uma nova amizade em uma rede social é mais provável de se concretizar quando os dois usuários em questão possuem amigos em comum, ou seja, quando ocorre fechamento triádico (RAPOPORT, 1953; BIANCONI et al., 2014; HUANG et al., 2015; BRANDT; LESKOVEC, 2014). Isso corrobora o entendimento de que as redes sociais não são formadas aleatoriamente (NEWMAN, 2003b). A Figura 3 ilustra uma rede de amizades caracterizada pela frequente formação de triângulos entre os nós.

Figura 3 – Estrutura de uma rede de amizades



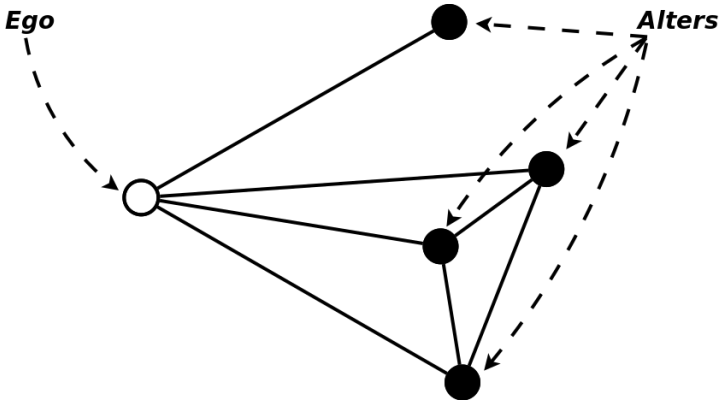
Fonte: Adaptado de Easley e Kleinberg (2010)

2.2.2.3 ***Ego-network***

Ego-network consiste na rede de amizades de uma pessoa. O nó central é chamado de *ego* e seus amigos são denominados de *alters*. Além dos nó *ego* e dos nós *alters*, complementam essa rede as conexões entre eles. Em outras palavras, *ego-network* seria a rede de amizades de um usuário considerando também as amizades entre seus amigos (LESKOVEC; MCAULEY, 2012). Dessa forma, pode-se entender que uma rede social é formada por n *ego-networks*, em que n seria o número de participantes da rede social. A Figura 4 ilustra uma *ego-newtwork* em que se vê o *ego*, os *alters* e suas conexões.

[4] *Microsoft Instant Mensenger*: programa de mensagens instantâneas que foi muito popular na primeira década deste século.

Figura 4 – Ilustração de uma *ego-network*



Fonte: Elaborado pelo autor

2.3 *Crowdsourcing*

Crowdsourcing é um conceito que consiste na realização de alguma tarefa com a colaboração de um grande número de pessoas, geralmente por meio da *Internet* (HOWE, 2006). Aplicações de *croudsourcing* visam resolver um problema de forma descentralizada explorando a diversidade do conhecimento humano (BRABHAM, 2008).

Cada vez mais pesquisas científicas têm utilizado *crowdsourcing* para rotular bases de dados (LIU et al., 2016; ZHAI et al., 2012; PARRY; TSAI, 2012), contudo, exemplos de diversas naturezas podem ser citados. O Waze[5], aplicativo que auxilia navegação no trânsito, recebe colaborativamente informações de trajetos e eventos de trânsito dos seus usuários. A Wikipédia[6], uma enciclopédia aberta, conta com a colaboração dos seus usuários para a geração e revisão de conteúdos. Na engenharia de *software*, *crowdsourcing* tem sido utilizado para desenvolvimento e testes de software (LATOZA; HOEK, 2016). *Crowdfunding*, conceito derivado de *crowdsourcing*, consiste na arrecadação colaborativa de recursos para financiar projetos, geralmente eventos e ações de caridade (BELLEFLAMME; LAMBERT; SCHWIENBACHER, 2014).

2.4 Gamificação

Gamificação consiste em utilizar elementos e princípios de jogos em contextos que não são jogos (DETERDING et al., 2011). A motivação para se aplicar a gamificação em alguma atividade ou produto visa aumentar o engajamento dos participantes e usuários (ZICHERMANN; CUNNINGHAM, 2011).

Chou (2015) sugere que combinar sentimentos de ansiedade, perda, motivação, recompensa e satisfação faz com jogos e soluções gamificadas consigam maior engajamento dos

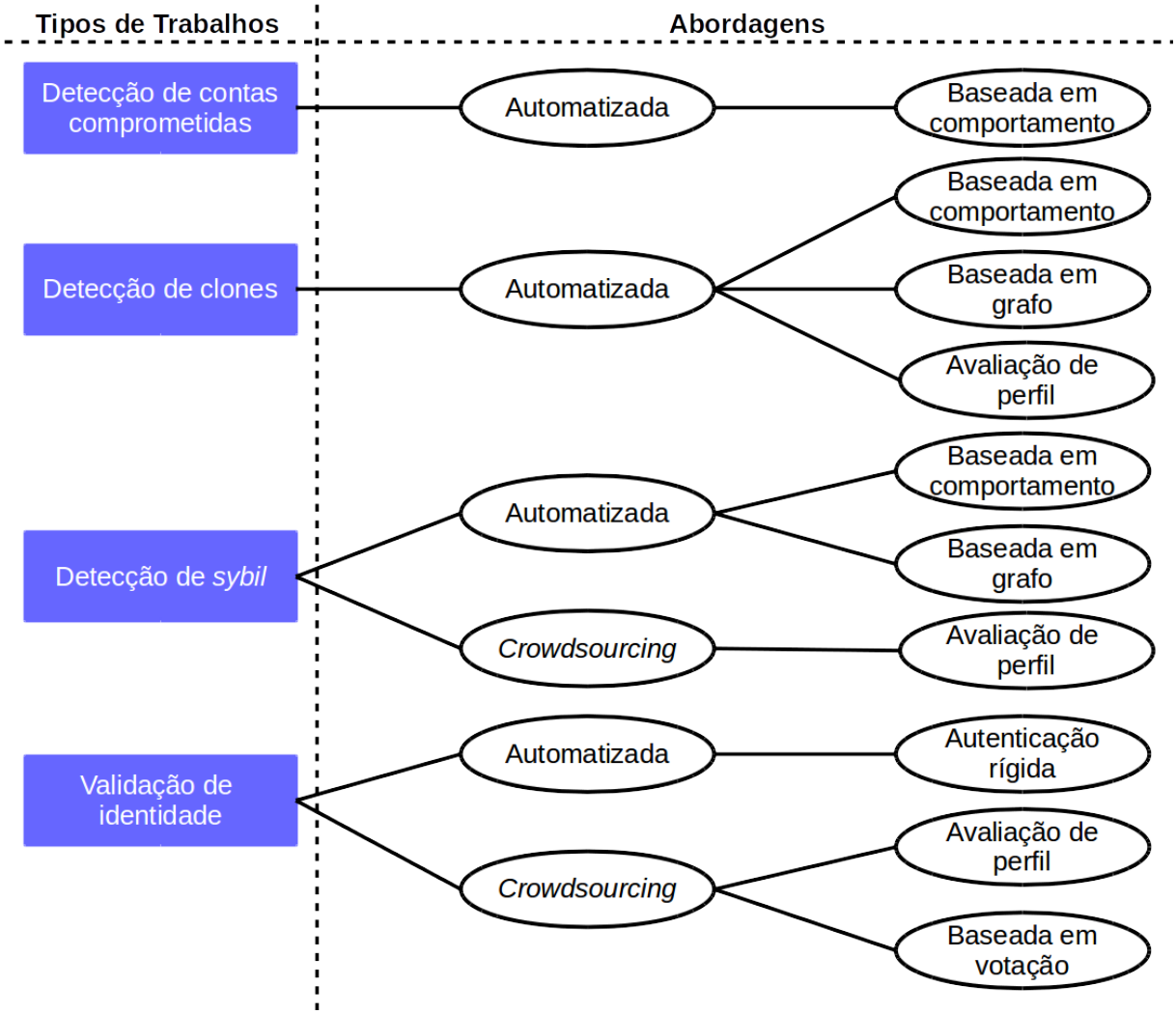
[5]https://www.waze.com
[6]https://wikipedia.org

usuários. Portanto, o autor considera que o ponto de partida para gamificar algo deve ser definir um significado para motivar o usuário a vencer todas as etapas. Recursos como pontos, medalhas, *rankings*, mudar de fase, progredir de nível e prêmios devem ser utilizados no sentido de estimular esses sentimentos.

3 TRABALHOS RELACIONADOS

Foi realizada revisão da literatura considerando trabalhos que visam identificar, combater e/ou validar usuários maliciosos presentes nas redes sociais *on-line*. Quatro tipos de trabalhos para esses fins foram identificados, conforme sintetizado na Figura 5 que adapta caracterização proposta por Bahri, Carminati e Ferrari (2016).

Figura 5 – Tipos de trabalhos e abordagens para combater usuários maliciosos de rede social *on-line*



Fonte: Adaptado de Bahri, Carminati e Ferrari (2016)

As abordagens adotadas nesta área de conhecimento permeiam os diferentes tipos de trabalhos, sendo que as abordagens mais exploradas na literatura são as baseada em grafo, baseada no comportamento do usuário e avaliação do perfil. As abordagens baseadas em grafo analisam características da topologia da rede para alcançar seus objetivos, enquanto que as abordagens baseadas no comportamento do usuário verificam características de navegação dos usuários e utilização dos recursos das redes sociais. As abordagens que consideram a avaliação do perfil buscam identificar usuários maliciosos com base em características presentes nos atributos de perfil (BAHRI; CARMINATI; FERRARI, 2016).

Os trabalhos de detecção de contas comprometidas basicamente utilizaram abordagens baseadas no comportamento do usuário. É o caso de Keretna, Hossny e Creighton (2013) que identificaram contas comprometidas a partir do padrão de digitação de texto. Bohacik, Fuchs e Benedikovic (2017) propuseram modelo de detecção de contas comprometidas que observa mudanças repentinas no comportamento de um usuário que tenta fazer *login* em uma conta. Mais frequentemente os trabalhos que objetivam detectar contas comprometidas observam padrão de navegação dos usuários (SHAHABADKAR; KAMATH; SHAHABADKAR, 2016; YADAV; CHATUR, 2017; RUAN et al., 2016; EGELE et al., 2017).

Para identificação de contas clonadas é comum se avaliar os perfis dos usuários a fim de se identificar similaridade dos atributos de perfil (JIN; TAKABI; JOSHI, 2011; BRÓDKA; SOBAS; JOHNSON, 2014). Contudo, visando diferenciar o perfil real do perfil clonado, trabalhos têm propostos modelos seguindo abordagem que verifica característica das redes dos usuários (KHAYYAMBASHI; RIZI, 2013; BRÓDKA; SOBAS; JOHNSON, 2014; JIN; TAKABI; JOSHI, 2011). Outra abordagem empregada por trabalhos que visam identificar perfis clonados consistem em verificar características do padrão de acesso e comportamento de navegação dos usuários (KIRUTHIGA; KANNAN et al., 2014; SHAN et al., 2013).

Os trabalhos de detecção de *sybils* são os que apresentam literatura mais vasta. A abordagem mais clássica para esse fim é analisar a topologia da rede em que se presume que usuários honestos tendem a formar uma rede *fast mixing*, ou seja, uma rede em que os nós honestos rapidamente formam um componente gigante densamente conectado, enquanto que esta propriedade não ocorre para os *sybils*, pois esses teriam dificuldades em consolidar amizades com os usuários reais. Com isso, assume-se que os grafos das redes sociais formam regiões distintas entre usuários honestos e *sybils*. Trabalhos que empregam essa abordagem clássica comumente implementam o algoritmo *Random Walks* para detectar as regiões honestas e falsas da rede social. Tal técnica consiste em construir caminhos aleatórios em um grafo e com isso detectar um indicador de conectividade dos nós para em seguida encontrar regiões que sejam mais ou menos densas (RAMALINGAM; CHINNAIAH, 2018; KOLL et al., 2014). Exemplos de *frameworks* que seguem metodologia baseada em grafo são SybilGuard (YU et al., 2008), SybilInfer (DANEZIS; MITTAL, 2009), SybilShield (VISWANATH et al., 2010), SybilLimit (YU et al., 2010), Facebook Immune System (STEIN; CHEN; MANGLA, 2011), SybilRank

(YANG; CAO; SIRIVIANOS, 2012), SybilDefender (WEI et al., 2013), SybilBelief (GONG; FRANK; MITTAL, 2014), Íntegro (BOSHMAF et al., 2016), SybilRadar (MULAMBA; RAY; RAY, 2016) e SybilSCAR (WANG; ZHANG; GONG, 2017).

Outros trabalhos que visam a detecção de ataques *sybils* aplicaram abordagens relacionadas ao comportamento dos usuários. Nesse sentido, Wang et al. (2013), Yang et al. (2014), Cao et al. (2014), Yadav e Chatur (2017), Wang et al. (2017) utilizaram análise de padrões de navegação dos usuários para encontrar *sybils*. Já os modelos propostos em Gong, Frank e Mittal (2014), Laleh, Carminati e Ferrari (2015), Li et al. (2016), Al-Qurishi et al. (2018) implementaram uma combinação de técnicas que consideram abordagem baseada em grafo com abordagem baseada no comportamento do usuário.

Wang et al. (2012) apontam que as abordagens automatizadas baseadas em grafo e no comportamento dos usuários não seriam eficazes contra ataques *sybils* sofisticados, eles propõem solução baseada em *crowdsourcing* que explora o conhecimento de humanos para avaliar o perfil do usuário e com isso identificar *sybils*.

Enquanto os trabalhos de detecção de *sybils* visam descobrir em larga escala se um conjunto de usuários são reais ou falsos, por sua vez, os trabalhos de validação de identidade analisam cada usuário individualmente e verificam a veracidade da identidade declarada (BAHRI; CARMINATI; FERRARI, 2018).

Uma abordagem conservadora para validação de identidade é a realização de uma autenticação rígida dos usuários, em que o provedor de um serviço emprega verificação física de documentos, certificados digitais e/ou biometria. Pode-se citar como exemplo dessa abordagem o banco Nubank[1] que realiza cadastro de novos clientes totalmente pela *Internet* por meio do envio de documentos digitalizados. No Brasil o e-CPF[2] consiste em um certificado digital utilizado para autenticação em serviços da Receita Federal e mais recentemente foi lançado o Documento Nacional de Identidade (DNI)[3] que se propõe ser uma identidade digital do cidadão e permitir autenticação em serviços públicos e privados. O Tribunal Superior Eleitoral (TSE) também tem adotado abordagem de autenticação rígida ao incorporar verificação biométrica nas urnas eletrônicas[4]. Serviços de natureza financeira e governamental aplicam autenticação rígida dos usuários visando reduzir os riscos de fraudes, entretanto, essa abordagem não é conveniente para as redes sociais *on-line* e outros serviços da *Internet* em razão das características de escala global e também pela intenção em se ter um processo de cadastramento simples para atrair o maior número possível de usuários.

Nesse sentido, trabalhos têm proposto abordagens menos rígidas para produzir uma nota que indique o nível de confiabilidade de um usuário de rede social *on-line*. Uma das abordagens consiste em avaliar o perfil do usuário para determinar sua nota de confiabilidade. Seguindo

[1] https://www.nubank.com.br
[2] http://idg.receita.fazenda.gov.br/contato/fale-conosco/cidadao/certificacao-digital
[3] http://www.dni.gov.br/
[4] http://www.tse.jus.br/eleitor/biometria/biometria

essa abordagem, Soliman et al. (2015, 2016), Bahri, Carminati e Ferrari (2016) propuseram modelos que se baseiam na aprendizagem de correlações entre atributos de perfil e no uso de *crowdsourcing* para avaliar coerências de padrões de perfis dos usuários. Sirivianos et al. (2014) propôs o sistema FaceTrust que emprega uma abordagem baseada em votação para determinar níveis de confiabilidade dos atributos de perfil de usuários de redes sociais *on-line*. No FaceTrust os avaliadores são os próprios amigos dos usuários avaliados.

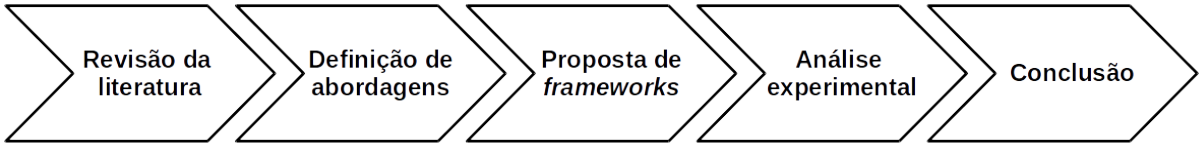
Neste trabalho, pretende-se analisar experimentalmente abordagens para validação de atributos de perfil de usuários de redes sociais *on-line*. Foram encontrados na literatura trabalhos seguindo diferentes abordagens para combater diferentes tipos de usuários maliciosos, entretanto, o FaceTrust (SIRIVIANOS et al., 2014) foi o único trabalho encontrado que valida atributos de perfil em específico; os demais trabalhos visavam validar o perfil do usuário por inteiro. Neste trabalho é proposto e avaliado experimentalmente o *framework MyFriends-Checker* (Seção 4.1) que sugere modificações ao FaceTrust, tais como medidas para dificultar conluio entre usuários e aplicação de gamificação para aumentar o engajamento dos usuários.

Não foram identificados na literatura trabalhos que utilizam abordagem baseada em grafo para validação de atributos de perfil de usuários de rede social *on-line*. Visando explorar adequação de abordagem baseada em grafo para validação de atributos de perfil neste trabalho também foi proposto e avaliado experimentalmente o *framework EgoNetwork-Checker* (Seção 4.2) que considera fenômenos comuns nas redes sociais para determinar um indicador do nível de confiabilidade para cada atributo do perfil de um usuário.

4 *FRAMEWORKS* PROPOSTOS

Neste capítulo são apresentados os *frameworks* propostos neste trabalho bem como a metodologia considerada. A Figura 6 apresenta uma visão geral das etapas realizadas neste trabalho. A primeira etapa foi a realização de uma revisão da literatura dos trabalhos que propuseram metodologias para identificar, combater e/ou validar usuários maliciosos de redes sociais *on-line* (Capítulo 3).

Figura 6 – Metodologia adotada



Fonte: Elaborado pelo autor

Na revisão da literatura identificaram-se as principais abordagens para validação da identidade de usuário de rede social *on-line*. Este trabalho propõe *frameworks* e analisa experimentalmente duas dessas abordagens. Na Seção 4.1, é apresentado o *framework EgoNetwork-Checker* que considera uma abordagem baseada na verificação da coerência dos atributos de perfil de um usuário com sua rede de amizades. E na Seção 4.2, é apresentado o *framework MyFriends-Checker* que considera uma abordagem baseada no *feedback* dos amigos por meio de um sistema de votação. No Capítulo 5 são apresentados experimentos realizados para esses *frameworks* e no Capítulo 6 são apresentadas as conclusões obtidas com este trabalho.

Cabe destacar que foram empregados procedimentos metodológicos de pesquisa experimental para atingir os objetivos estabelecidos neste trabalho. Classifica-se como um trabalho de natureza aplicada no qual se empreenderam práticas que seguem uma abordagem quantitativa, em que análises estatísticas foram consideradas para compreensão dos resultados obtidos.

4.1 *Framework EgoNetwork-Checker*

O *framework* aqui denominado *EgoNetwork-Checker* é baseado em um trabalho preliminar desenvolvido pelos autores (LIMA; MARQUES-NETO, 2018). Este *framework* aplica a abordagem de validação da identidade de um usuário de rede social *on-line* por meio da verificação da coerência dos seus atributos de perfil com sua rede de amizades.

O *EgoNetwork-Checker* foi formulado considerando algumas premissas relacionadas a fenômenos comuns das redes sociais, descritas na Seção 4.1.1. Na Seção 4.1.2, métricas de *ego-network* foram definidas visando medir os fenômenos considerados nessas premissas. Em síntese, o *EgoNetwork-Checker* utiliza métricas de *ego-network* para determinar níveis de confiabilidade dos atributos de perfil de usuários de redes sociais *on-line*, conforme apresentado na Seção 4.1.3. O experimento realizado para avaliar a aplicabilidade do *EgoNetwork-Checker* é descrito na Seção 5.1.

4.1.1 Premissas

O *EgoNetwork-Checker* assume como premissas as ocorrências dos fenômenos de homofilia e fechamento triádico nas *ego-networks* dos usuários honestos, pois, conforme se constata na literatura, esses são fenômenos comuns nas redes sociais.

A ideia considerada no *EgoNetwork-Checker* é que a *ego-network* de um usuário é coerente com seus atributos de perfil. Com base nisso, é esperado que, se um nó *ego* tiver um atributo específico, consequentemente ele irá se conectar a algum grupo de nós *alters* que também tenha esse mesmo atributo. Além disso, como as conexões sociais não são criadas aleatoriamente, espera-se que este grupo de nós *alters* represente uma rede caracterizada por níveis mais elevados de homofilia e agrupamento de usuários.

As características de homofilia e fechamento triádico já foram observadas no contexto das *ego-networks* (LESKOVEC; MCAULEY, 2012; WEN; YUAN, 2016). O escopo da *ego-network* foi considerado importante para elaboração do *EgoNetwork-Checker*, pois esse é o menor conjunto de dados de uma rede social *on-line* que permite caracterizar as propriedades de formação de homofilia e comunidade envolvendo um determinado usuário.

4.1.2 Métricas de ego-network

O *EgoNetwork-Checker* considera métricas que visam expressar a coerência de um atributo de perfil de um usuário de rede social *on-line* com sua *ego-network*. O primeiro passo para calcular essas métricas é encontrar o conjunto de nós *alters* que possui o mesmo atributo de perfil do nó *ego* a ser verificado. Neste trabalho, este conjunto é referenciado como S_i, em que i indica o atributo de perfil verificado. A seguir são listadas as métricas definidas:

- n_i: $|S_i|$, ou seja, o número de nós *alters* que possuem i;
- h_i: coeficiente de homofilia calculado para i considerando uma rede composta por todos nós *alters* que declararam algum atributo de perfil;
- g_i: coeficiente de agrupamento médio para uma rede composta por nós de S_i.

No *EgoNetwork-Checker*, h_i corresponde ao coeficiente de homofilia proposto por Newman (2003a) (Equação 2.3). A métrica g_i determina o coeficiente de agrupamento médio de uma rede formada exclusivamente pelos nós que compõem S_i e suas arestas. A Equação 4.1 apresenta o cálculo para a métrica g_i, em que f representa a função que calcula o coeficiente de agrupamento de um determinado nó.

$$g_{\mathrm{i}} = \frac{1}{n_{\mathrm{i}}} \sum_{j=1}^{n_{\mathrm{i}}} f(S_{\mathrm{i}}[j]) \tag{4.1}$$

4.1.3 Definição do framework

Esta seção apresenta como o *framework EgoNetwork-Checker* define um nível de confiabilidade t_i para cada atributo i que compõe o perfil de um usuário de rede social *on-line*. O *EgoNetwork-Checker* é baseado nas métricas n_i, h_i e g_i. O cálculo de t_i está relacionado aos valores de desvio padrão e média dessas métricas, além dos pesos das métricas que são estabelecidos no Módulo 1 deste *framework* (Seção 4.1.3.1). O segundo e último módulo deste *framework* (Seção 4.1.3.2) é onde se obtêm os valores de t_i. Neste *framework*, t_i pode assumir valores de 0 até 1; a ideia é que quanto mais próximo de 1 maior é a confiabilidade de um atributo de perfil ser verdadeiro; e quanto mais próximo de 0 menor é a confiabilidade de um atributo de perfil ser verdadeiro.

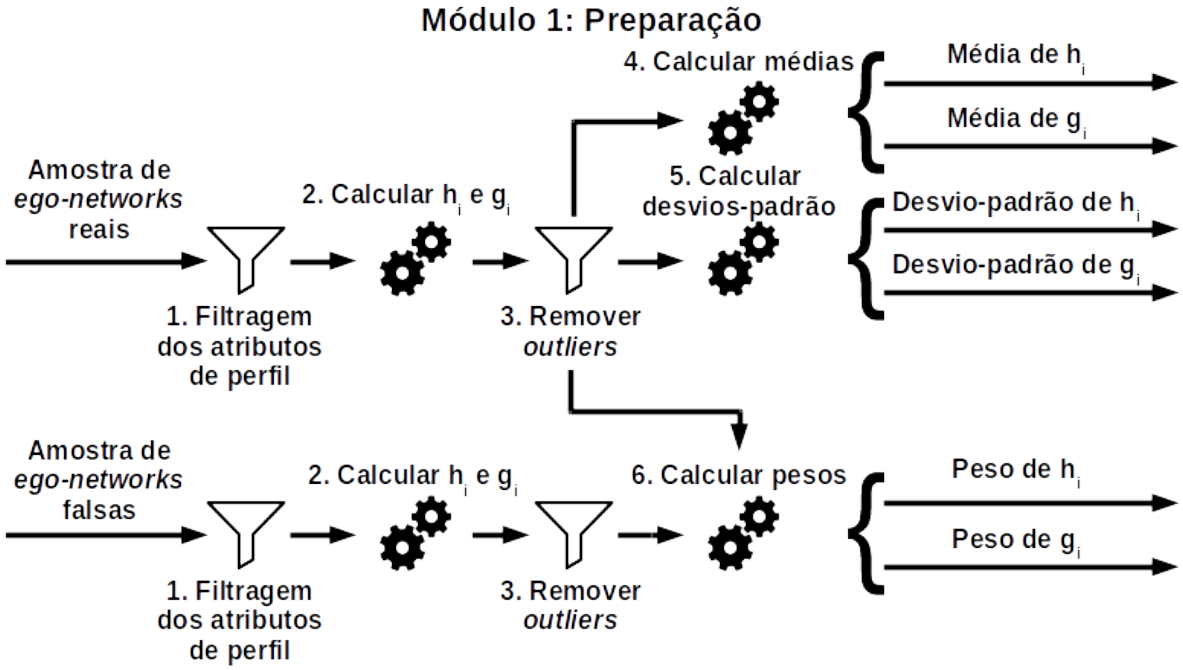
Este *framework* foi proposto visando permitir flexibilização na sua aplicação, por isso, nesta seção os procedimentos são apresentados apenas conceitualmente. Opções de implementação são detalhadas na Seção 5.1, em que o *framework* foi experimentalmente aplicado.

4.1.3.1 Módulo 1: Preparação

O primeiro módulo consiste em calcular os valores de referência que serão utilizados no módulo seguinte. Para aplicar este *framework* é necessário selecionar uma amostra de *ego-networks* de usuários reais, na qual os atributos de perfil selecionados dos usuários são reconhecidamente verdadeiros. Também é necessário selecionar uma amostra de *ego-networks* de usuários com atributos de perfil falsos. Essas duas amostras consistem nos parâmetros de entrada do Módulo 1, conforme ilustrado na Figura 7.

A primeira etapa deste módulo trata de filtrar os atributos de perfil dos nós *egos*, consistindo na definição de um valor mínimo de n_i. Em seguida, na etapa 2, as métricas h_i e g_i são calculadas para os atributos de perfil dos nós *egos*. Na terceira etapa, os valores *outliers* devem ser removidos para reduzir as distorções causadas por atributos de perfil que possuem métricas com comportamento extremamente fora dos padrões das amostras. Todas essas três etapas iniciais são executadas paralelamente na amostra de usuários reais e na amostra de usuários falsos.

Figura 7 – Primeiro módulo do *EgoNetwork-Checker*



Fonte: Elaborado pelo autor

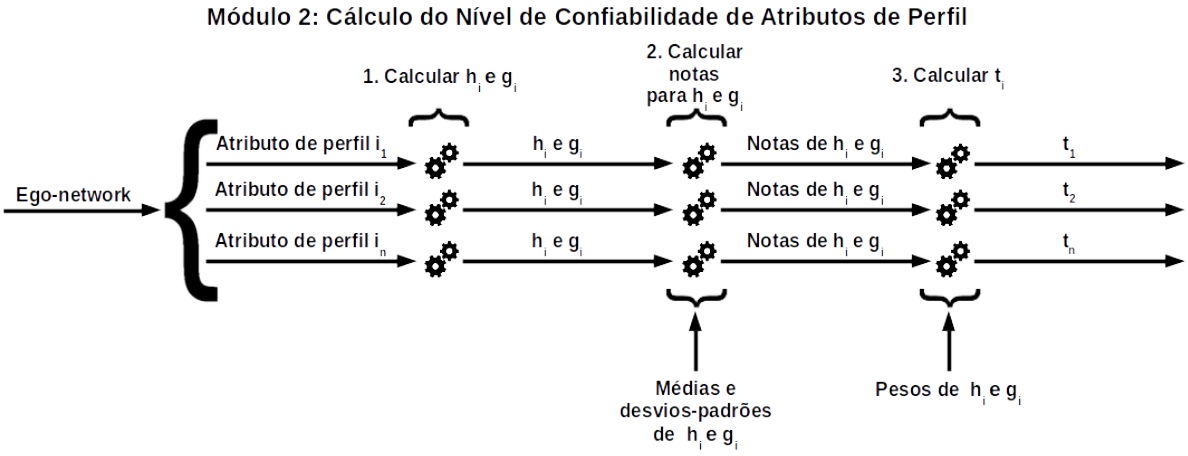
Na quarta etapa deste módulo são calculadas as médias das métricas h_i e g_i considerando a amostra de usuários reais. Na penúltima etapa realizam-se os cálculos dos desvios-padrão para as métricas h_i e g_i também considerando apenas a amostra de usuários reais. Por fim, a última etapa deste módulo consiste em calcular os pesos atribuídos a cada uma das métricas. Esses pesos devem refletir a importância de cada métrica para determinar o valor de t_i para um atributo de perfil i. O cálculo desses pesos consideram tanto a amostra real como a amostra falsa de *ego-networks*. A soma dos pesos deve ser igual a 1 por motivo de normalização.

4.1.3.2 Módulo 2: Cálculo do nível de confiabilidade de atributos de perfil

O segundo módulo deste *framework* consiste no cálculo dos valores de t_i para cada atributo de perfil de um usuário. Conforme ilustrado na Figura 8, os parâmetros recebidos neste módulo são a *ego-network* de um usuário e os valores resultantes do Módulo 1.

Para cada atributo de perfil i de um nó *ego* é calculado o valor de t_i correspondente. Para isso, o primeiro passo consiste em calcular os valores de h_i e g_i para os atributos de perfil do nó *ego* em avaliação. Depois, uma nota entre 0 e 1 é definida para cada uma das métricas h_i e g_i. O Algoritmo 1 calcula uma nota para uma métrica em que se recebe como parâmetro de entrada o valor da métrica em questão. Outros dois parâmetros de entrada do Algoritmo 1 correspondem à média e ao desvio-padrão relacionados a essa métrica, ambos calculados no Módulo 1. A nota é definida proporcionalmente dentro de um intervalo de valores, em que os limites inferior e superior são definidos, respectivamente, nas linhas 1 e 2 do algoritmo.

Figura 8 – Segundo módulo do *EgoNetwork-Checker*



Fonte: Elaborado pelo autor

Algoritmo 1 Cálculo da nota de uma métrica de *ego-network*

Entrada: valor v, média avg e desvio-padrão sd de uma métrica de *ego-network*
Saída: nota de uma métrica de *ego-network*

1: $bottom \leftarrow avg - sd$
2: $top \leftarrow avg + sd$
3: $amplitude \leftarrow top - bottom$
4: **se** $v < bottom$ **então retorna** 0
5: **fim se**
6: **se** $v > top$ **então retorna** 1
7: **fim se**
8: **retorna** $(v - bottom)/amplitude$

O passo final para calcular t_i de um atributo de perfil consiste em ponderar as notas das métricas h_i e g_i com seus respectivos pesos que foram definidos no *Módulo 1* deste *framework*. O valor de t_i de um atributo de perfil é dado pela Equação 4.2, em que sh_i e sg_i são as notas das métricas h_i e g_i, respectivamente; e wh e wg correspondem aos pesos de h_i e g_i, respectivamente.

$$t_i = (sh_i * wh) + (sg_i * wg) \tag{4.2}$$

4.2 *Framework MyFriends-Checker*

O *framework MyFriends-Checker* aplica abordagem apoiada no *crowdsourcing* para validação dos atributos de perfil de um usuário de rede social *on-line*. Este *framework* adota estratégia que consiste em considerar a opinião dos amigos para determinar os níveis de confiabilidade dos atributos de perfil de um usuário em avaliação. As premissas consideradas para formulação deste *framework* são apresentadas na Seção 4.2.1, e em seguida, na Seção 4.2.2, o *framework* é apresentado. O experimento realizado para avaliar a aplicabilidade do *MyFriends-Checker* é descrito na Seção 5.2.

4.2.1 Premissas

O *MyFriends-Checker* assume que os usuários de uma rede social *on-line* sabem responder perguntas sobre os atributos de perfil dos seus amigos. Também é esperado que a maioria dos usuários respondam honestamente perguntas sobre seus amigos.

4.2.2 Definição do framework

Esta seção apresenta como o *framework MyFriends-Checker* define um nível de confiabilidade t_i para cada atributo i que compõe o perfil de um usuário u de rede social *on-line*. O *MyFriends-Checker* considera a opinião dos amigos de u para determinar t_i, que assim como no *EgoNetwork-Checker* pode assumir valores de 0 até 1; em que quanto mais próximo de 1 maior é a confiabilidade de um atributo de perfil ser verdadeiro; e quanto mais próximo de 0 menor é a confiabilidade de um atributo de perfil ser verdadeiro.

Este *framework* foi proposto visando permitir flexibilização na sua aplicação; por isso, nesta seção os procedimentos são apresentados apenas conceitualmente. Opções de implementação são detalhadas na Seção 5.2, em que o *framework* foi experimentalmente aplicado.

O primeiro passo do *MyFriends-Checker* para avaliar um atributo de perfil consiste em selecionar avaliadores. Esses avaliadores são selecionados entre os amigos do usuário em avaliação e devem atender a critérios de credibilidade. Para cada avaliador o *MyFriends-Checker* deve atribuir um peso que represente a credibilidade daquele avaliador para responder o questionamento em questão.

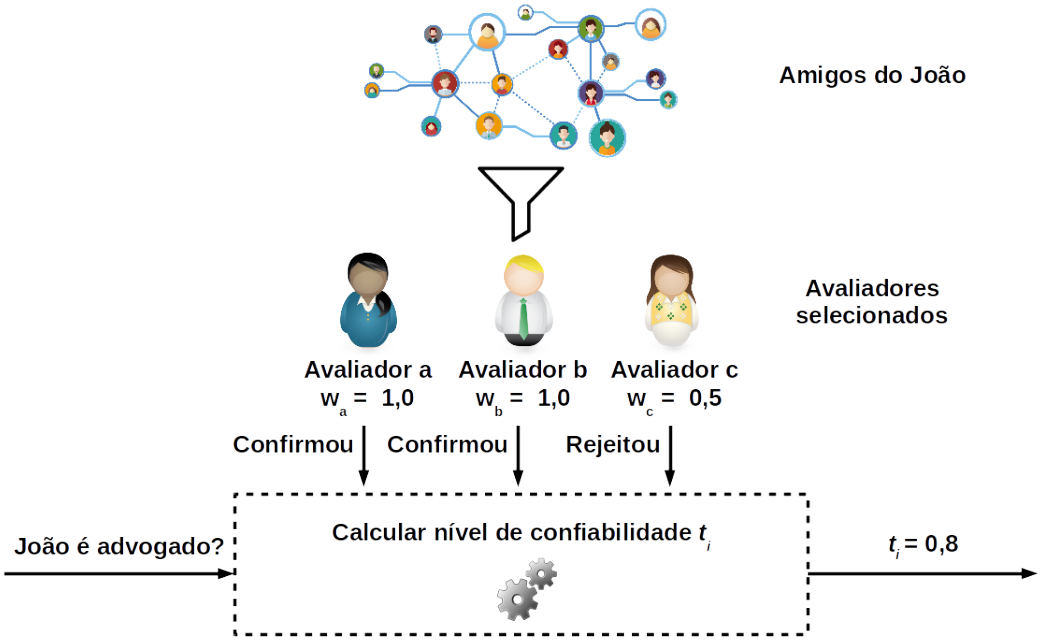
O *MyFriends-Cheker* deve apresentar aos avaliadores um conjunto de opções de respostas, estando o atributo de perfil em avaliação neste conjunto. Além dessas opções de respostas, os avaliadores também podem responder que nenhuma das opções é verdadeira ou que não sabe responder a pergunta. Desta forma, é considerado que o avaliador confirmou o atributo de perfil em avaliação quando ele selecionar a mesma opção declarada pelo usuário em avaliação. O avaliador rejeita o atributo de perfil em avaliação quando ele seleciona opção diferente da informada pelo usuário em avaliação ou quando seleciona que nenhuma das opções é verdadeira. Quando o avaliador responde que não sabe, sua avaliação é ignorada do cálculo de t_i.

Para fins de cálculo do t_i, considera-se que uma resposta assume valor igual a 1 (um) quando ela confirma o atributo de perfil em avaliação e assume valor igual a 0 (zero) quando ela rejeita o atributo de perfil em avaliação. O cálculo do t_i consiste numa média ponderada considerando o peso do avaliador e sua resposta. A Equação 4.3 expressa como se obtém t_i para cada atributo i que compõe o perfil de um usuário, onde n corresponde ao número de avaliadores, A_i corresponde a um vetor com as respostas dos avaliadores e W_i corresponde a um vetor com os pesos dos avaliadores.

$$t_i = \frac{\sum_{j=1}^{n} (A_i[j] * W_i[j])}{\sum_{j=1}^{n} W_i[j]} \tag{4.3}$$

Para exemplificar o funcionamento do *MyFriends-Checker*, considere que *João* seja um usuário de rede social e que ele autodeclarou em seu perfil que trabalha como advogado. A Figura 9 apresenta uma exemplificação de como seria a validação da profissão do *João* por meio *MyFriends-Checker*.

Figura 9 – Exemplo da validação de um atributo de perfil no *MyFriends-Checker*



Fonte: Elaborado pelo autor

5 ANÁLISE EXPERIMENTAL DOS *FRAMEWORKS*

Neste capítulo os *frameworks* propostos foram experimentalmente analisados utilizando amostras reais de rede social *on-line*. Na Seção 5.1 e na Seção 5.2 os experimentos realizados para os *frameworks* EgoNetwork-Checker e MyFriends-Checker são apresentados, respectivamente.

5.1 *Framework EgoNetwork-Checker*

Nesta seção é apresentado experimento realizado com o *framework EgoNetwork-Checker*. Primeiro, foram definidas amostras de dados para serem utilizadas no experimento, Seção 5.1.1. Em seguida, as características dos dados considerados neste experimento são apresentadas na Seção 5.1.2. A implementação e análise dos resultados são apresentadas na Seção 5.1.3.

5.1.1 Definição das amostras de dados

Neste experimento foram utilizados dados reais da rede social Google+, coletados por Gong et al. (2012). Os autores relatam ter coletado atributos de perfil e conexões de aproximadamente 75% do total de usuários do Google+ em outubro de 2011. Os atributos de perfil coletados são do tipo cidade, empresa, escola e profissão.

Uma amostra de dados composta por 99.792 *ego-networks* foi selecionada a partir dos dados coletados por Gong et al. (2012) e neste trabalho será referenciada como *Amostra Real*. O critério para definição da *Amostra Real* consistiu numa filtragem de *ego-networks* de nós *egos* que tivessem algum atributo de perfil declarado e no mínimo 100 amigos, considerando apenas as conexões recíprocas. Ao todo, a *Amostra Real* possui 4.135.327 usuários, 54.682.803 conexões recíprocas e 6.057.953 atributos de perfil, sendo que 509.201 são atributos de perfil dos nós *egos*.

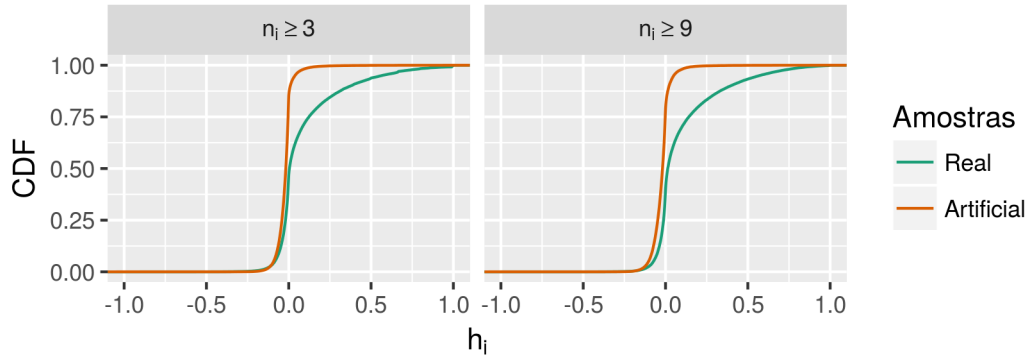
Além da *Amostra Real*, neste experimento também foi gerada sinteticamente uma amostra chamada de *Amostra Artificial*. A *Amostra Real* é a base para a construção da *Amostra Artificial*, sendo que a amostra gerada sinteticamente possui o mesmo grafo da amostra original. O que diferencia essas duas amostras é que na *Amostra Artificial* os atributos de perfil dos nós *alters* de cada *ego-network* foram redistribuídos aleatoriamente. A *Amostra Artificial* é relevante para este experimento porque permite confrontar as métricas oriundas de *ego-networks* reais com as métricas de *ego-networks* geradas aleatoriamente. A utilização de amostras sintéticas aleatórias é prática recorrente em trabalhos de validação de usuários de redes sociais *on-line* (LALEH; CARMINATI; FERRARI, 2017; SOLIMAN et al., 2016; TRAN et al., 2011; MULAMBA; RAY; RAY, 2016).

5.1.2 Características das amostras de dados

Nesta seção são analisadas as métricas de *ego-network* dos atributos de perfil dos nós *egos* das amostras de dados consideradas neste experimento. Métricas como h_i e g_i somente fazem sentido de ser analisadas quando há n_i no mínimo igual a três, pois esse valor de n_i corresponde à menor quantidade de nós que permite a formação de um triângulo. Constatou-se que apenas 20% dos atributos de perfil das amostras possuem n_i maior ou igual a três. Presume-se que quanto maior o valor de n_i mais significativos são os valores de h_i e g_i, entretanto, quanto maior n_i menor é o conjunto de atributos de perfil a ser analisado. Por exemplo, para n_i mínimo igual a nove apenas 9% dos atributos de perfil das amostras seriam considerados.

A Figura 10 apresenta a Função de Distribuição Cumulativa (CDF) de h_i para cenário considerando atributos de perfil com n_i mínimo igual a três e para cenário em que se desconsideram atributos de perfil em que n_i é menor que nove. Nos dois cenários analisados, o valor de h_i dos atributos de perfil da *Amostra Real* tende a ser superior aos valores observados para os atributos de perfil da *Amostra Artificial*. Quando o n_i mínimo é três o h_i médio é igual a 0,0897 na *Amostra Real* e -0,0218 na *Amostra Artificial*. Para n_i mínimo igual a 9 o valor médio de h_i da *Amostra Real* eleva para 0,0999 e o valor médio de h_i *Amostra Artificial* reduz para -0,0226.

Figura 10 – Distribuição de h_i nas amostras de dados considerando $n_i \geqslant 3$ e $n_i \geqslant 9$

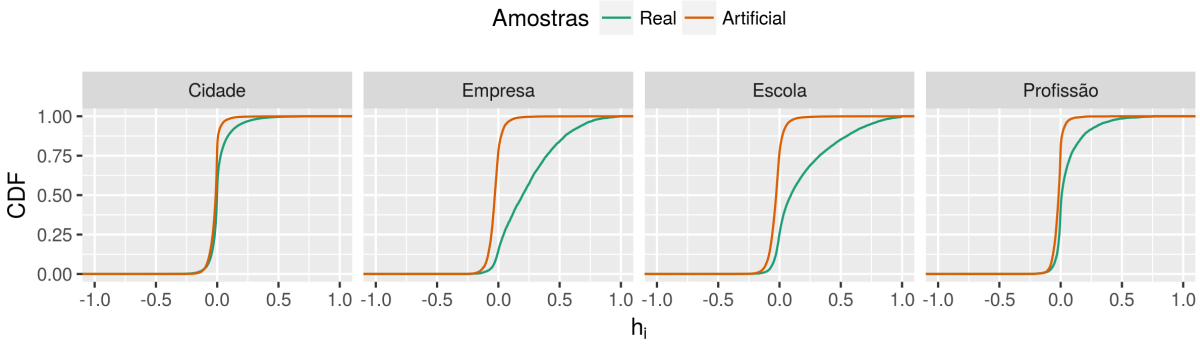


Fonte: Elaborado pelo autor

Foi constatado que o nível de homofilia varia de acordo com o tipo de atributo de perfil. Conforme apresentado na Figura 11 os atributos do tipo empresa e escola da *Amostra Real* apresentam valores de h_i maiores que nos atributos do tipo cidade e profissão.

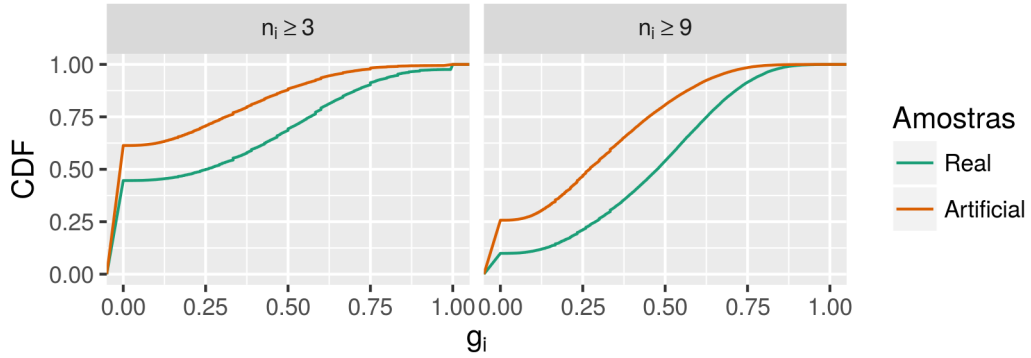
A Figura 12 apresenta CDF em relação à métrica g_i da *Amostra Real* e da *Amostra Artificial* em cenários com n_i mínimo igual a três e com n_i mínimo igual a nove. Em ambos os cenários se constata que os atributos de perfil da *Amostra Real* alcançam g_i maiores em relação à *Amostra Artificial*. Também é possível perceber que significativa fração de atributos de perfil obtiveram g_i igual a zero quando se considera cenário com n_i mínimo igual a três. No cenário com n_i mínimo igual a nove o número de atributos de perfil com g_i igual a zero é drasticamente reduzido.

Figura 11 – Distribuição de h_i por tipo de atributo de perfil nas amostras de dados considerando $n_i \geqslant 9$



Fonte: Elaborado pelo autor

Figura 12 – Distribuição de g_i nas amostras de dados considerando $n_i \geqslant 3$ e $n_i \geqslant 9$



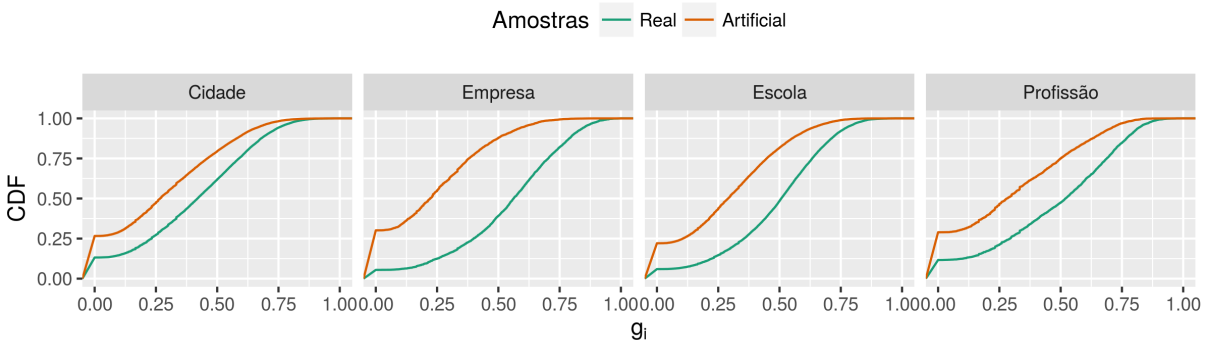
Fonte: Elaborado pelo autor

Assim como h_i varia de acordo com o tipo de atributo de perfil, g_i também apresenta características específicas de acordo com o tipo de atributo de perfil, conforme apresentado na Figura 13. Na *Amostra Real* os valores médios obtidos para de g_i foram 0,401, 0,534, 0,480 e 0,475 respectivamente para os atributos de perfil do tipo cidade, empresa, escola e profissão. Na *Amostra Artificial* os valores médios obtidos para de g_i foram 0,280, 0,234, 0,290 e 0,297 respectivamente para os atributos de perfil do tipo cidade, empresa, escola e profissão.

5.1.3 Implementação do framework e análise dos resultados

O *EgoNetwork-Checker* foi executado considerando as amostras de dados definidas na Seção 5.1.1, entretanto, a *Amostra Real* foi dividida em 2 partes com a mesma quantidade de *ego-networks*, gerando a *Amostra Real*$_1$ e *Amostra Real*$_2$. A mesma metodologia foi aplicada à *Amostra Artificial*, dando surgimento à *Amostra Artificial*$_1$ e à *Amostra Artificial*$_2$. O objetivo é utilizar a *Amostra Real*$_1$ e a *Amostra Artificial*$_1$ no primeiro módulo do *EgoNetwork-Checker*, que é o módulo de preparação. A *Amostra Real*$_2$ e a *Amostra Artificial*$_2$ foram utilizadas no segundo módulo do *framework* que é quando se calcula o t_i dos atributos de perfil.

Figura 13 – Distribuição de g_i por tipo de atributo de perfil nas amostras de dados considerando $n_i \geqslant 9$



Fonte: Elaborado pelo autor

Pelo fato de ter sido constatado na Seção 5.1.2 que os indicadores de homofilia e agrupamento de usuários variam de acordo com o tipo do atributo de perfil, decidiu-se executar o *EgoNetwork-Checker* quatro vezes, uma vez para cada tipo de atributo de perfil. Isso implica que o resultado do *Módulo 1* será específico para os tipos de atributo de perfil cidade, empresa, educação e trabalho.

No *Módulo 1*, os parâmetros de entrada do *amostra de ego-networks reais* e *amostra de ego-networks falsas* corresponderam aos dados da *Amostra Real*$_1$ e *Amostra Artificial*$_1$, respectivamente. Na primeira etapa do *Módulo 1* é demandada a definição de n_i mínimo para a filtragem de atributos de perfil. O valor de n_i mínimo igual a 9 foi definido, considerando constatações observadas na Seção 5.1.2.

A segunda etapa do *Módulo 1* consistiu nos cálculos de h_i e g_i para os atributos de perfil dos nós *egos* das amostras. Na etapa 3 foram utilizados diagramas *boxplot* para inspecionar e remover *outliers* em relação às métricas h_i e g_i. Os valores de quartil 1 *Q1*, quartil 3 *Q3* e o intervalo interquartil *IQR* foram usados para calcular os limites inferiores e superiores para remoção de *outliers*. Foi considerado o limite inferior igual a $Q1-(1{,}5*IQR)$ e o limite superior igual a $Q3+(1{,}5*IQR)$ (SILVA; PERES; BOSCARIOLI, 2016). Ao todo 1.867 (8,63%) e 2.988 (13,80%) atributos de perfil com valores *outliers* de h_i e g_i foram removidos das amostras *Amostra Real*$_1$ ou *Amostra Artificial*$_1$, respectivamente.

Após a remoção de *outliers* foram executadas as etapas 4, 5 e 6 do Módulo 1 do *framework*. Na etapa 6, que é a etapa em que se calculam os pesos das métricas, foi utilizado o algoritmo *RandomForests* (BREIMAN, 2001) que tem como função identificar a importância das *features* (h_i e g_i no contexto deste trabalho) dentro de uma amostra com dados classificados. Os valores obtidos por meio do algoritmo *RandomForests* foram ponderados para que a soma dos pesos das métricas h_i e g_i seja igual a 1, conforme é especificado na etapa 6 do primeiro módulo do *framework*.

A Tabela 1 apresenta os resultados do primeiro módulo do *EgoNetwork-Checker*, onde se nota que a homofilia média para os atributos do tipo empresa e escola foram mais elevados e que a homofilia média para os atributos do tipo cidade e profissão ficaram próximos à linha de base zero. Os resultados médios em relação ao coeficiente de aglomeração também foram maiores para os atributos do tipo empresa e escola do que os atributos do tipo cidade e profissão. Também se nota que o peso da métrica relacionada à homofilia é maior que o peso da métrica relacionada ao coeficiente de aglomeração para todos os tipos de atributos, o que indica que a homofilia teve uma importância maior para determinar atributos de perfil verdadeiros e falsos da *Amostra Real*$_1$ e *Amostra Artificial*$_1$.

Tabela 1 – Resultados do *Módulo 1* do *EgoNetwork-Checker* para os atributos de perfil do tipo cidade, empresa, escola e profissão

Métrica		Cidade	Empresa	Escola	Profissão
h_i	Média	-0,001	0,238	0,176	0,022
	Desvio-padrão	0,036	0,232	0,232	0,064
	Peso	0,538	0,655	0,640	0,586
g_i	Média	0,422	0,536	0,476	0,469
	Desvio-padrão	0,235	0,228	0,212	0,262
	Peso	0,462	0,345	0,360	0,414

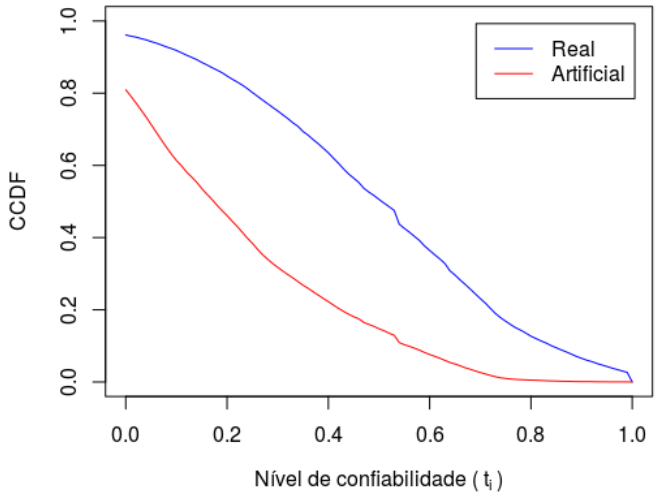
Fonte: Elaborado pelo autor

Os resultados apresentados na Tabela 1 consistem nos parâmetros de entrada do *Módulo 2* do *framework* proposto. O *Módulo 2* foi executado para cada um dos atributos de perfil dos nós *egos* que compõem a *Amostra Real*$_2$ e a *Amostra Artificial*$_2$. Como resultado foi obtido valor de t_i para cada um dos atributos de perfil considerados nesse módulo. Isso consiste no nível de confiabilidade que o *framework* atribui ao atributo de perfil analisado.

A Figura 14 exibe gráfico da Função de Distribuição Cumulativa Complementar (CCDF) de t_i nas amostras consideradas neste trabalho. Constata-se que em geral os níveis de confiabilidade são mais elevados para os atributos de perfil da *Amostra Real*$_2$ que para os atributos de perfil da *Amostra Artificial*$_2$, sendo que 50% dos atributos de perfil da *Amostra Real*$_2$ obtiveram t_i maior ou igual a 0,5 enquanto 85% dos atributos de perfil da *Amostra Artificial*$_2$ não alcançaram esse valor.

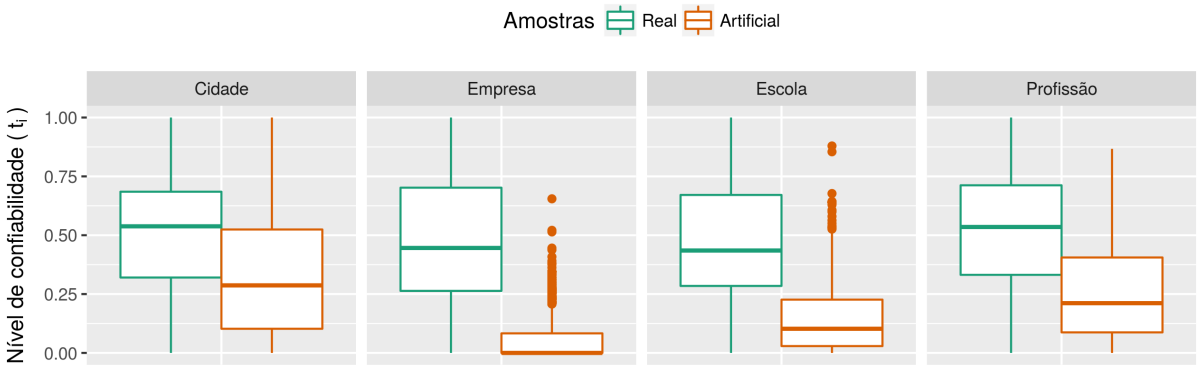
Neste experimento os atributos de perfil da *Amostra Real*$_2$ do tipo cidade e profissão obtiveram valores médio de t_i maiores que os atributos de perfil do tipo empresa e escola. Por sua vez o inverso foi constatado ao se analisar os atributos de perfil da *Amostra Artificial*$_2$. A Figura 15 apresenta gráficos *boxplot* nos quais os atributos de perfil do tipo empresa e escola são mais facilmente distinguíveis entre *Amostra Real*$_2$ e *Amostra Artificial*$_2$ que os atributos de perfil do tipo cidade e profissão.

Figura 14 – Distribuição de t_i nas amostras de dados



Fonte: Elaborado pelo autor

Figura 15 – Distribuição de t_i por tipo de atributo de perfil nas amostras de dados



Fonte: Elaborado pelo autor

É importante destacar que as amostras de dados deste experimento não possuem *ground truth* assegurado. Essa limitação atualmente afeta qualquer trabalho que precise coletar dados de rede e perfil de usuários de redes sociais *on-line*, pois os termos de uso dos serviços mais populares restringem uso de *crawlers* e suas *Application Programming Interface* (API) oficiais permitem acesso limitado aos dados. Para evitar essa limitação em trabalhos futuros será necessário ter acesso à amostras de dados de redes sociais *on-line* com informações rotuladas sobre os usuários.

5.1.4 Análise da complexidade

As métricas n_i, h_i e g_i tiveram seus custos de execução analisados. Essas métricas são calculadas considerando o atributo i e a rede formada com os nós *alters* da *ego-network* do usuário u, que é quem possui i. Portanto, nesta seção, considere que as arestas do grafo em questão é representado por uma matriz de adjacências formada por nós *alters*.

Para determinar n_i é necessário verificar quais nós *alters* possuem i; desta forma, o custo é $O(a)$, em que a é o número de nós *alters* da *ego-network* de u. O cálculo de h_i verifica quantas arestas ligam pares de nós que possuem i; assim seu comportamento assintótico é $O(a^2)$.

A métrica g_i consiste no coeficiente de *clustering* médio do subconjunto S_i dos nós *alters* que possuem i. Desse modo, o tempo de execução para calcular g_i é dado por $O(s^3)$, em que s é o número de elementos de S_i.

5.2 *Framework MyFriends-Checker*

Nesta seção é apresentado experimento realizado com o *framework MyFriends-Checker*. Primeiro é descrita a implementação do *MyFriends-Quiz* que consiste no *front-end* do *MyFriends-Checker*, Seção 5.2.1. Na Seção 5.2.2 são apresentadas características dos usuários que participaram do *MyFriends-Quiz* durante o período deste experimento. Em seguida, o *ground truth* do epxerimento é apresentado na Seção 5.2.3. A implementação do *framework* é detalhada na Seção 5.2.4. Na Seção 5.2.5 o custo de execução do *framework* é analisado. É importante destacar que o *MyFriends-Checker* é inspirado na metodologia proposta pelo FaceTrust (SIRIVIANOS et al., 2014); desta forma, a Seção 5.2.6 apresenta as modificações sugeridas neste trabalho.

5.2.1 MyFriends-Quiz

Neste trabalho foi desenvolvido o *MyFriends-Quiz* que é um jogo de perguntas e respostas entre usuários do Facebook, disponível no endereço *https://myfriends-quiz.com*. Ele foi desenvolvido para possibilitar a experimentação do *framework MyFriends-Checker* e atende às especificações definidas na Seção 4.2.2.

A elaboração e desenvolvimento do *MyFriends-Quiz* agregou conceitos de *crowdsourcing* e gamificação. Ele é uma implementação de *crowdsourcing*, pois consiste em um solução colaborativa para que usuários de uma rede social avaliem uns aos outros. Recursos de gamificação foram incorporados visando aumentar o engajamento dos usuários com o sistema. Com isso, o sistema foi projetado na forma de um jogo de perguntas e respostas, além de possuir funcionalidades de pontuação, níveis de evolução dos usuários, prêmios internos ao evoluir de nível, *ranking*, mensagens motivacionais e *feedback* constante aos usuários.

O *MyFriends-Quiz* possui dois tipos de perguntas: (i) sobre atributos de perfil de amigos e (ii) sobre o tipo de relacionamento com um amigo ou amigo indireto (amigo de amigo). O usuário que participa do *MyFriends-Quiz* responde esses tipos de perguntas sobre seus amigos e vice-versa. Para participar do *MyFriends-Quiz* o usuário deve fazer *login* com sua conta do Facebook e autorizar compartilhamento da sua rede de amizades e dos seus atributos de perfil com o *MyFriends-Quiz*. Importante destacar que, conforme termos de serviço da API do Facebook, na época de desenvolvimento do sistema, somente é fornecido o compartilhamento das conexões de amizade entre usuários em que ambos estejam participando do *MyFriends-Quiz*.

As perguntas sobre atributos de perfil consideram foto do perfil, gênero do usuário, faixa etária, cidade natal, cidade atual, histórico de estudo, histórico de trabalho, status de relacionamento e gênero de interesse. Sendo que, devido à natureza do tipo de atributo de perfil, as alternativas de respostas podem ser um conjunto de opções fixas ou um conjunto de opções dinâmicas. Possuem conjunto de opções de respostas fixas os atributos de perfil do tipo faixa etária, status de relacionamento, gênero do usuário e gênero de interesse. Os atributos de perfil do tipo foto do perfil, cidade natal, cidade atual, histórico de estudo e histórico de trabalho possuem conjunto de opções de respostas dinâmicas gerado a partir de uma base de dados previamente definida. A Figura 16a e a Figura 16b foram extraídas do *MyFriends-Quiz* e exemplificam como as perguntas sobre atributos de perfil são apresentadas aos usuários.

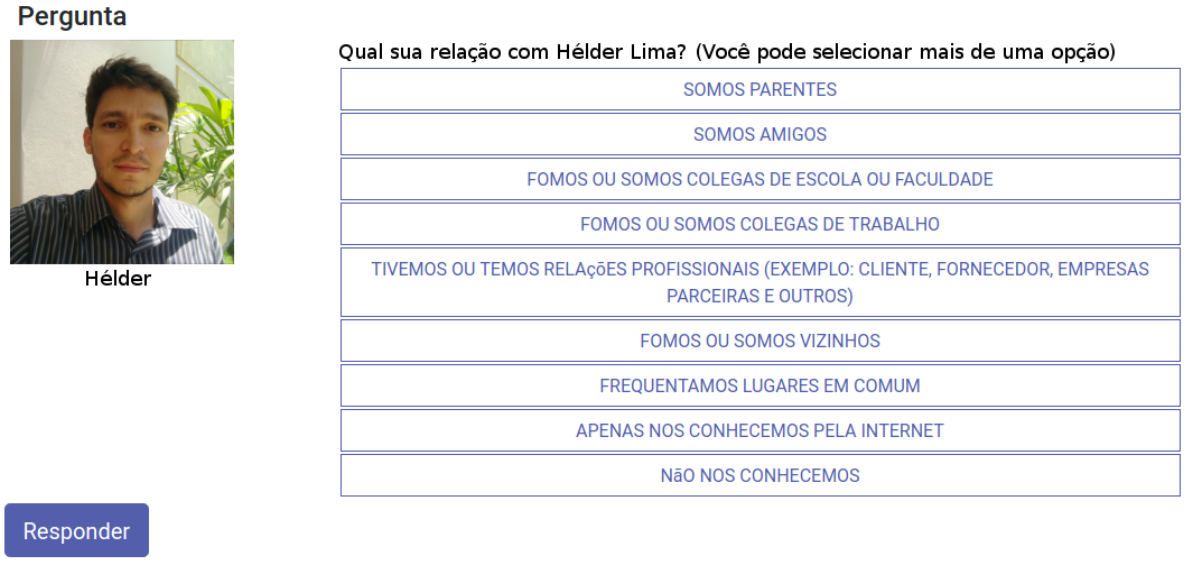
Figura 16 – Exemplos de perguntas do *MyFriends-Quiz* sobre atributos de perfil
(a)Pergunta sobre status de relacionamento (b)Pergunta sobre cidade natal

Fonte: Elaborado pelo autor

As perguntas sobre atributos de perfil têm o objetivo de verificar a veracidade do perfil autodeclarado pelos usuários de rede social. Já as perguntas sobre o tipo de relacionamento entre usuários examinam a existência do indivíduo na sociedade. As perguntas sobre tipo de relacionamento sempre exibem o mesmo conjunto de opções de reposta e visam extrair o contexto social envolvido nas amizades dos usuários, conforme exemplo de pergunta ilustrado na Figura 17.

A forma como esses dois tipos de perguntas é utilizado pelo *framework* é explicado na Seção 5.2.4. É importante destacar que para mitigar conluio entre os usuários o *MyFriends-Quiz* estabelece um tempo máximo de resposta para cada pergunta, e um avaliador nunca pode responder duas vezes a mesma pergunta sobre o mesmo usuário. O *MyFriends-Quiz* também não permite que o avaliador escolha quem irá avaliar e vice-versa.

Figura 17 – Exemplo de pergunta do *MyFriends-Quiz* sobre tipo de relacionamento entre usuários



Fonte: Elaborado pelo autor

5.2.2 Usuários do MyFriends-Quiz

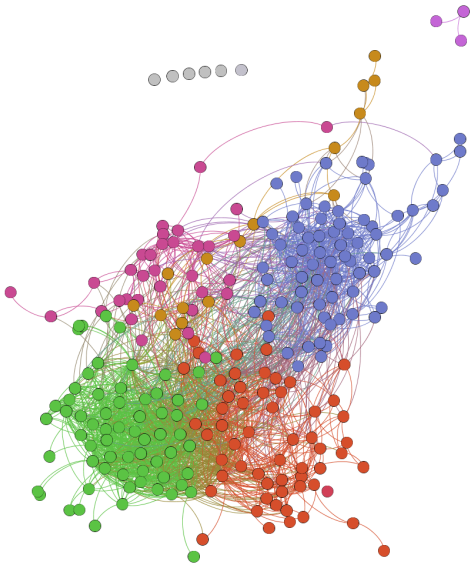
O *MyFriends-Quiz* foi lançado no dia 20/03/2018. Os dados considerados neste experimento correspondem da data do lançamento do sistema até o dia 30/03/2018, período em que o *MyFriends-Quiz* foi divulgado para alunos do Instituto Federal do Norte de Minas Gerais Campus Januária. Todos os usuários que participaram do *MyFriends-Quiz* consentiram em fornecer seus dados para este experimento ao estar de acordo com os termos desse serviço[1]. Ao todo 253 usuários do Facebook participaram do *MyFriends-Quiz*, resultando numa rede com 2.386 conexões de amizades (Figura 18) e 2.020 atributos de perfil.

5.2.2.1 Características da rede

A rede de usuários do *MyFriends-Quiz* é uma rede bem conectada, sendo que possui componente gigante com 243 usuários (96% do total de usuários). O diâmetro da rede é 7, entretanto, o caminho médio entre os nós é 2,56. O grau médio da rede é 18,86 e a densidade do grafo é 0,075. As cores da Figura 18 representam comunidades identificadas por meio do algoritmo proposto por Blondel et al. (2008) e apresentadas com o auxílio da ferramenta Gephi[2]. Ao todo 13 comunidades foram identificadas, e o indicador de modularidade é 0,41.

[1] https://myfriends-quiz.com/politica_privacidade.php
[2] https://gephi.org/

Figura 18 – Rede de usuários do *MyFriends-Quiz*



Fonte: Elaborado pelo autor

5.2.2.2 Características dos nós

A Tabela 2 apresenta a quantidade e porcentagem de usuários do *MyFriends-Quiz* que possuem tipos específicos de atributos de perfil. Constata-se que todos os usuários declararam no Facebook foto do perfil, faixa etária e gênero. Informações sobre cidade natal e atual foram declaradas por mais de 90% dos usuários. Atributos de perfil sobre educação foram declarados por 82% dos usuários, sendo quase o dobro da quantidade de usuários que declararam atributos de perfil sobre trabalho.

Tabela 2 – Quantidade e porcentagem de usuários do *MyFriends-Quiz* que possuem atributos de perfil

Tipo de atributo	# de usuários	% usuários
Foto do perfil	253	100
Faixa etária	253	100
Gênero do usuário	253	100
Cidade atual	237	94
Cidade natal	229	91
Educação	208	82
Status de relacionamento	161	64
Trabalho	108	43
Gênero de interesse	80	32

Fonte: Elaborado pelo autor

A Tabela 3 apresenta os atributos de perfil mais frequentes entre os usuários do *MyFriends-Quiz*. Os atributos de perfil do tipo educação é o mais frequentemente declarado pelos usuários, sendo que os 253 usuários declararam no total 401 atributos sobre escola ou faculdade que frequentaram. O perfil predominante dos usuários do *MyFriends-Quiz* consiste em jovens de 18 até 29 anos, solteiros e estudantes. As cidades de nascimento e residência da maioria dos usuários é Januária ou cidades próximas, com exceção de São Paulo que é a cidade natal de 16 usuários.

O atributo de perfil do tipo trabalho merece atenção especial nesta pesquisa, uma vez que facilmente se percebe que usuários do *MyFriends-Quiz* declararam atributos de perfil falsos ou incorretos. A empresa *Estudante* foi a mais declarada pelos usuários, entretanto esta empresa não existe, do que se deduz que esses usuários desejaram expressar que sua ocupação é estudar. As empresas *Frases & Versos*[3] e *Facebook* também foram declaradas por usuários, entretanto isso consiste numa sátira. *Frases & Versos* não é uma empresa, mas uma página do Facebook com conteúdo de humor que possui mais de cinco milhões de participantes, e nenhum dos oito usuários que declararam trabalhar na rede social *Facebook* trabalham de fato nesta empresa. Os usuários que declararam que trabalham nas empresas *Frases & Versos* e no *Facebook* foram questionados sobre qual a razão de declararem este atributo de perfil; todos afirmaram ser uma brincadeira. Observações em relação a esses atributos de perfil identificados como incorretos foram realizadas ao definir o *ground truth* do experimento, Seção 5.2.3, e também ao se analisar os resultados obtidos com a implementação do *framework*, Seção 5.2.4.

5.2.3 Ground truth

Nesta seção é apresentado o *ground truth* considerado neste experimento. Observações em relação aos dois tipos de perguntas do *MyFriends-Quiz* foram realizadas, desta forma, na Seção 5.2.3.1 e na Seção 5.2.3.2 se definem e se analisam amostras considerando atributos de perfil e tipos de relacionamentos, respectivamente.

5.2.3.1 Atributos de perfil

Foram selecionados 20 usuários do *MyFriends-Quiz* para compor o *ground truth* deste experimento. Os atributos de perfil desses usuários foram verificados e reconhecidos como verdadeiros. Neste experimento, os atributos de perfil desses usuários serão referenciados como *Amostra Real*.

[3]https://www.facebook.com/oficialsofrases/

Tabela 3 – Atributos de perfil mais comuns entre os usuários do *MyFriends-Quiz* por tipo

(a)Educação

Total de atributos de perfil	401
IFNMG	34%
Josefino Barbosa	6%
Olegário Maciel	4%
Claudemiro Alves Ferreira	3%
Outros	53%

(b)Trabalho

Total de atributos de perfil	153
Estudante	11%
IFNMG	8%
Frases & Versos	8%
Facebook	5%
Outros	68%

(c)Cidade natal

Total de atributos de perfil	229
Januária	38%
Itacarambi	11%
São Paulo	7%
Montes Claros	6%
Outros	38%

(d)Cidade atual

Total de atributos de perfil	237
Januária	55%
Itacarambi	12%
Pedras de Maria da Cruz	5%
Montes Claros	4%
Outros	24%

(e)Faixa etária

Total de atributos de perfil	253
De 18 até 29 anos	73%
Menos de 18 anos	18%
De 30 até 39 anos	7%
De 40 até 49 anos	2%

(f)Status de relacionamento

Total de atributos de perfil	161
Solteiro(a)	66%
Relacionamento sério	24%
Casado(a)	9%
Noivo(a)	1%

(g)Gênero de interesse

Total de atributos de perfil	80
Feminino	68%
Masculino	31%
Masculino e feminino	1%

(h)Gênero do usuário

Total de atributos de perfil	253
Masculino	51%
Feminino	49%

Fonte: Elaborado pelo autor

O objetivo deste experimento é avaliar se os amigos dos usuários da *Amostra Real* reconhecem os atributos de perfil verdadeiros desses usuários e também se reconhecem atributos de perfil falsos desses usuários. Para isso, foram injetados atributos falsos no perfil dos 20 usuários que compõem a *Amostra Real*. Esses atributos de perfil falsos foram selecionados aleatoriamente no banco de opções de respostas do *MyFriends-Quiz* e serão referenciados como *Amostra Falsa A*.

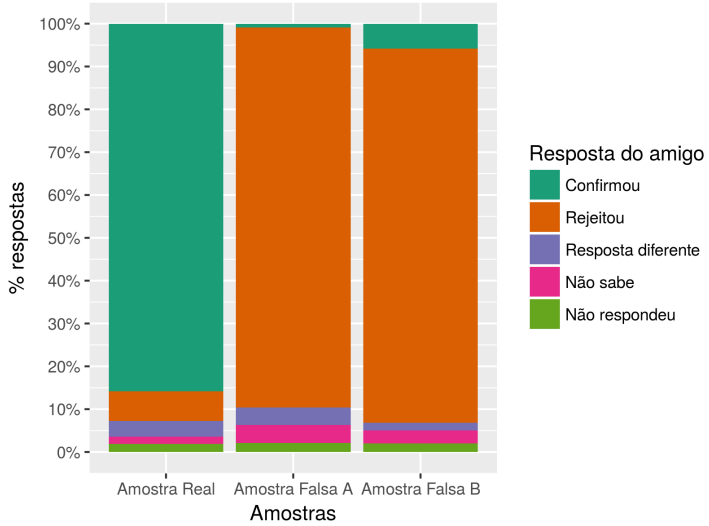
Uma terceira amostra denominada, *Amostra Falsa B*, também foi criada. Ela foi estruturada seguindo o mesmo princípio da *Amostra Falsa A*, entretanto, os atributos de perfil não foram definidos aleatoriamente e sim foram selecionados atributos de perfil comuns na região da Januária/MG, cidade de residência da maioria dos usuários do *MyFriends-Quiz*. O objetivo

é observar se os atributos de perfil da *Amostra Falsa B* serão reconhecidos como verdadeiros pelo fato de eles serem recorrentes entre os usuários do *MyFriends-Quiz*.

Destaca-se que tanto na *Amostra Falsa A* como na *Amostra Falsa B* foram injetados atributos de perfil apenas dos tipos que possuem conjunto de opções de respostas dinâmicas, ou seja, cidade natal, cidade atual, foto do perfil, educação e trabalho. Não foram injetados atributos do tipo faixa etária, gênero do usuário, gênero de interesse e status de relacionamento para não haver repetição de pergunta com as mesmas opções de respostas, pois o conjunto de opções de respostas desses atributos de perfil é fixo. Também cabe destacar que nenhum usuário teve seu perfil alterado no Facebook; a injeção de atributos de perfil falsos se restringiram ao contexto do *MyFriends-Quiz*.

Um total de 8.629 avaliações foram realizadas no *MyFriends-Quiz* considerando os atributos de perfil que compõem as *Amostra Real*, *Amostra Falsa A* e *Amostra Falsa B*. A Figura 19 mostra que aproximadamente 90% das avaliações confirmaram os atributos de perfil autodeclarados pelos usuários da *Amostra Real*. Por outro lado, nota-se grande rejeição dos atributos de perfil das amostras falsas. Esses resultados corroboram a premissa deste experimento que assume que os amigos de usuários de rede social sabem responder perguntas sobre seus atributos de perfil. Entretanto, cabe destacar que quando se comparam as avaliações dos atributos de perfil da *Amostra Falsa A* e *Amostra Falsa B*, fica evidenciado que ao injetar atributos de perfil populares da região dos usuários se alcança maior taxa de avaliação positiva, ainda que modestas, pois apenas cerca 1% das avaliações confirmaram os atributos de perfil da *Amostra Falsa A* e aproximadamente 6% das avaliações confirmaram os atributos de perfil da *Amostra Falsa B*.

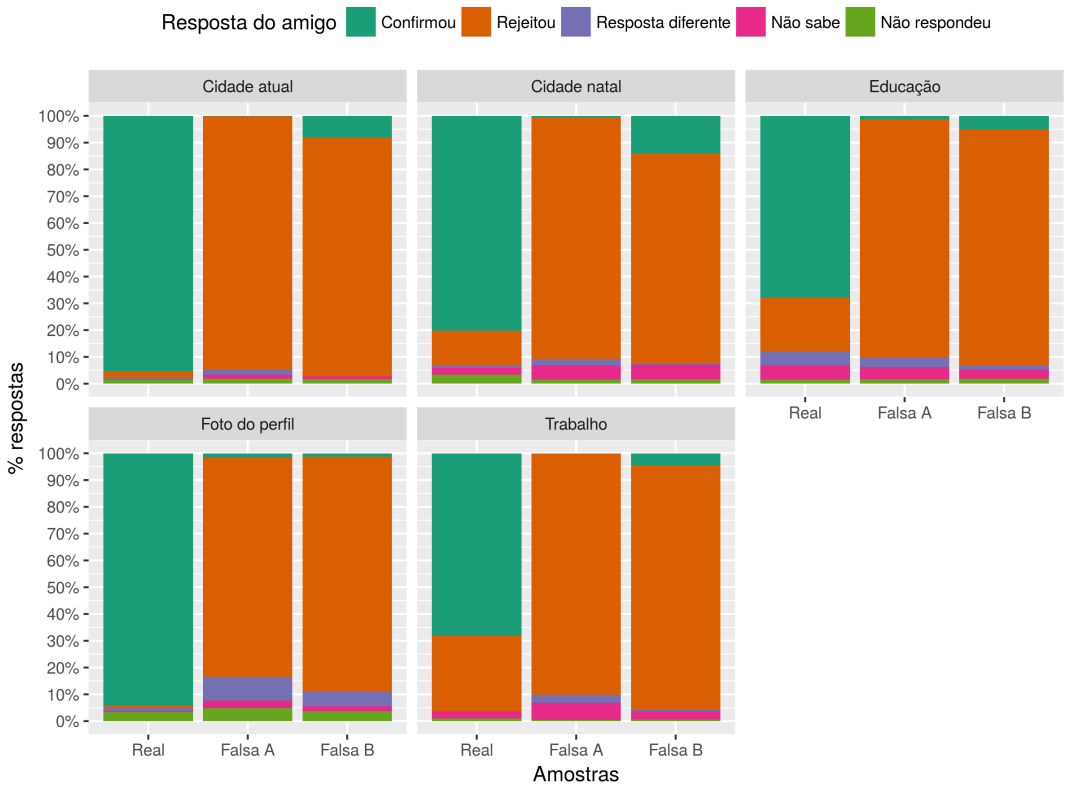
Figura 19 – Avaliação dos atributos de perfil no *MyFriends-Quiz*



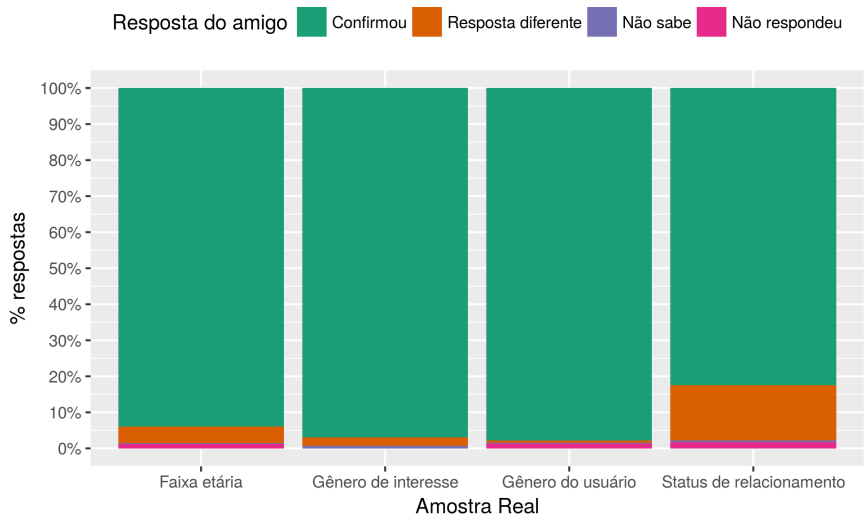
Fonte: Elaborado pelo autor

Figura 20 – Avaliações dos atributos de perfil no *MyFriends-Quiz* por tipo

(a)Atributos de perfil com opções de respostas dinâmicas



(b)Atributos de perfil com opções de respostas fixas



Fonte: Elaborado pelo autor

A Figura 20 apresenta as avaliações dos atributos de perfil por tipo. No caso da *Amostra Real* os atributos que possuem as menores porcentagens de confirmação são do tipo educação e trabalho com cerca de 70% de confirmações. Os atributos de perfil do tipo status de relacionamento da *Amostra Real* também obtiveram porcentagem de confirmações abaixo

da média, cerca de 83%, os demais tipos de atributos de perfil da *Amostra Real* obtiveram porcentagem de confirmação acima de 90%. Todos os tipos de atributos de perfil da *Amostra Falsa A* foram amplamente rejeitados, entretanto, os atributos de perfil da *Amostra Falsa B* do tipo cidade natal e cidade atual obtiveram relativo êxito em confirmações, aproximadamente 9% e 14%, respectivamente.

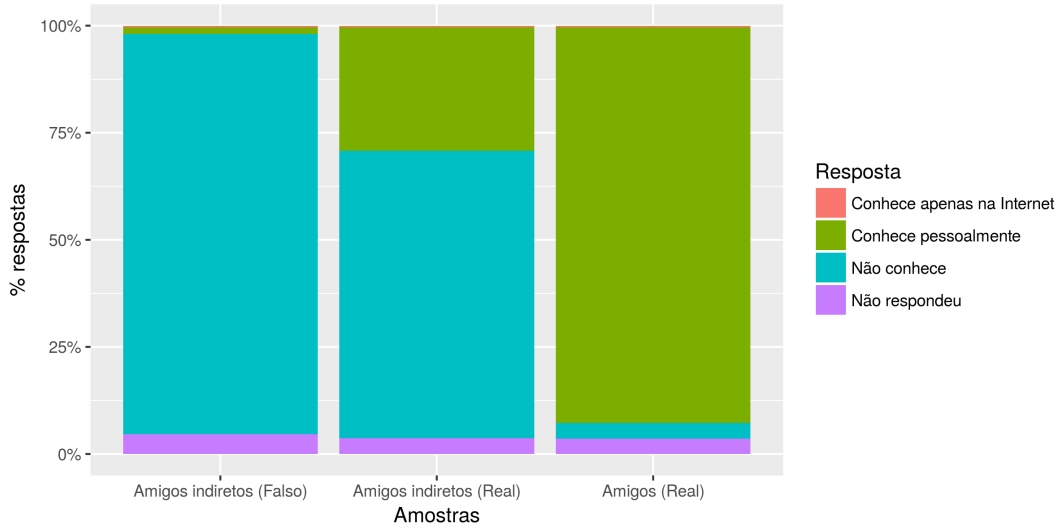
Apesar de os atributos de perfil do tipo trabalho da *Amostra Real* terem obtido taxas de confirmação abaixo da média, quando comparado com os demais tipos de atributo de perfil dessa mesma amostra, é possível constatar que a proporção de confirmações desses atributos é significativamente superior aos atributos de perfil identificados como falsos ou incorretos, conforme apresentado na Seção 5.2.2.2. Os atributos de perfil *Estudante*, *Frases & Versos* e *Facebook* foram confirmados em 47%, 36% e 23% das avaliações, respectivamente.

Os falsos negativos e falsos positivos observados nas avaliações dos usuários podem ser decorrentes de engano do avaliador ou caso de avaliador mal-intencionado que propositadamente respondia a opção errada. Para compreender melhor como o usuário do *MyFriends-Quiz* se comporta ao avaliar um amigo foi aplicado o questionário disponível no Apêndice A que contém uma questão sobre como o avaliador respondia as perguntas. Ao todo, 27 usuários do *MyFriends-Quiz* responderam o questionário e 59% informaram que selecionavam as respostas que pareciam mais óbvias, mesmo sem ter em certeza. Outros 41% informaram que somente respondiam quando tinham certeza. Isso indica que as implementações do *MyFriends-Checker* devem considerar o histórico de respostas dos avaliadores para determinar seu peso. O objetivo deve ser fazer com que os avaliadores que somente respondem quando têm certeza, e, portanto, irão errar menos, tenham maior influência no cálculo de t_i do que avaliadores que respondem mesmo sem ter certeza.

5.2.3.2 Tipo de relacionamento

O *MyFriends-Quiz* faz perguntas sobre o tipo de relacionamento entre amigos e também entre amigos indiretos (amigo de amigo). O objetivo é extrair o contexto social das amizades e até mesmo se os usuários conhecem de fato as pessoas próximas a ela numa rede social. Foram analisadas as avaliações atribuídas aos 20 usuários da *Amostra Real* definida na Seção 5.2.3.1. Para contrapor às observações das avaliações do tipo relacionamento dos usuários da *Amostra Real*, 20 usuários falsos foram criados. Esses usuários falsos não possuem amigos, mas foram simuladas amizades entre pares de usuários da *Amostra Real* e usuários falsos a fim de que os amigos dos usuários da *Amostra Real* avaliem o tipo de relacionamento com usuários falsos.

Figura 21 – Avaliações dos tipos de relacionamento entre usuários do *MyFriends-Quiz*



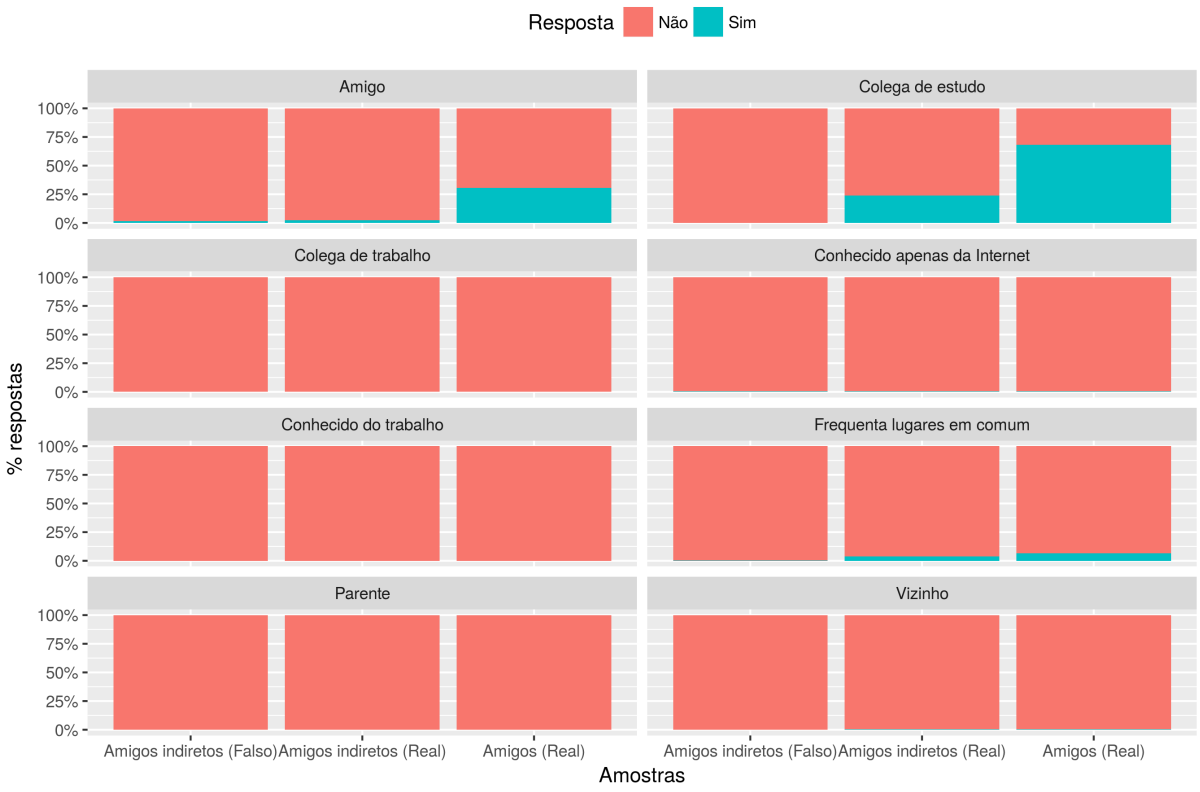
Fonte: Elaborado pelo autor

Um total de 784 avaliações foram realizadas no *MyFriends-Quiz* considerando os tipos de relacionamento dos usuários da *Amostra Real* e os usuários falsos. A Figura 21 mostra que 93% das avaliações feitas por amigos dos usuários da *Amostra Real* dizem se conhecerem pessoalmente e que 3,6% dizem não se conhecerem, mesmo eles sendo amigos no Facebook. Quando se analisam as amizades indiretas nota-se que 29% das avaliações indicam que se conhecem pessoalmente, mesmo esses usuários não sendo amigos diretos no Facebook. No caso dos usuários falsos 93% das avaliações indicaram desconhecer estes usuários.

A Figura 22 detalha os tipos de relacionamentos entre os usuários do *MyFriends-Quiz*. Os contextos educacional e de amizades predominam na maioria das conexões dos usuários da *Amostra Real*.

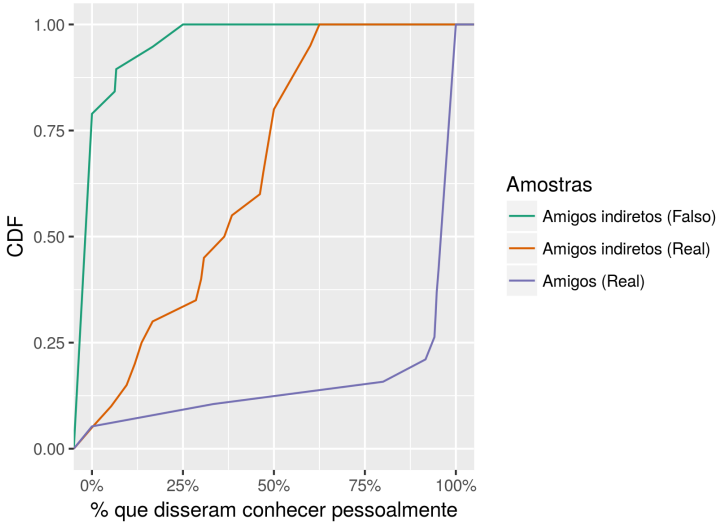
Algumas constatações podem ser tiradas após analisar as avaliações dos tipos de conexões, especialmente as ligações entre amigos indiretos. Ficou demonstrado que os usuários de rede social são conhecidos em alguma medida além da sua *ego-network*. Além disso, constata-se potencial de fechamento triádico entre os amigos indiretos, pois uma parcela deles já se conhecem pessoalmente mas ainda não concretizaram amizade no Facebook. A Figura 23 mostra que 75% dos usuários da *Amostra Real* são conhecidos por ao menos 12,5% dos seus amigos indiretos. Também se constata que cerca de 80% dos usuários falsos foram avaliados como desconhecidos por 100% dos seus avaliadores. Esses indicadores sugerem que a opinião dos amigos indiretos pode ser útil em um processo de validação de identidade de usuários de rede social *on-line*.

Figura 22 – Avaliações dos tipos de relacionamento entre usuários do *MyFriends-Quiz* detalhado



Fonte: Elaborado pelo autor

Figura 23 – Distribuição da porcentagem de amigos ou amigos indiretos que conhecem pessoalmente os usuários das amostras

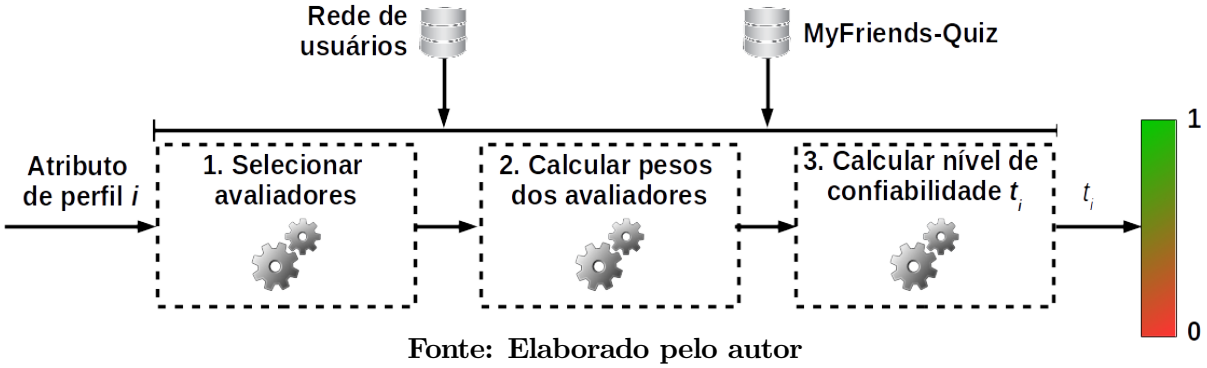


Fonte: Elaborado pelo autor

5.2.4 Implementação do framework e análise dos resultados

Nesta seção é descrita a implementação do *framework MyFriends-Checker* realizada neste experimento. O *MyFriends-Checker* foi executado para as *Amostra Real*, *Amostra Falsa A* e *Amostra Falsa B* definidas na Seção 5.2.3.1. Neste experimento o *MyFriends-Quiz* funcionou como uma fronteira de entrada de dados para o *MyFriends-Checker*, conforme sugere a Figura 24. Cada atributo de perfil das amostras consideradas neste experimento teve t_i calculado com base na rede de amizades do usuário e nas avaliações do *MyFriends-Quiz*.

Figura 24 – Modelo da implementação experimental do *MyFriends-Checker*



Fonte: Elaborado pelo autor

A primeira etapa para avaliar um atributo i que compõe o perfil do usuário u no *MyFriends-Checker* consiste em filtrar os amigos de u que estão aptos para serem avaliadores. Portanto, neste experimento foi considerado que u somente pode ser avaliado por usuários que sejam pessoalmente conhecidos por no mínimo 10% dos seus amigos indiretos. Essa decisão foi tomada com base na análise dos tipos de relacionamento dos usuários apresentada na Seção 5.2.3.2. O objetivo dessa medida é mitigar a influência de perfis com baixo reconhecimento social no cálculo de t_i.

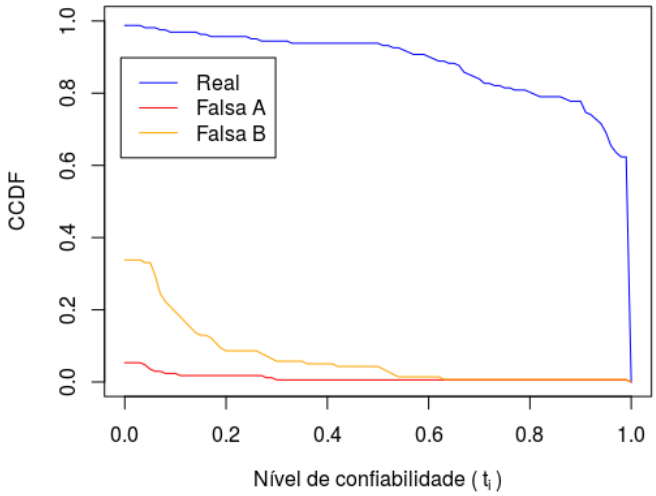
A segunda etapa consistiu em calcular os pesos dos avaliadores com base em seu histórico de avaliações de atributos de perfil do mesmo tipo de i. Desta forma, foi considerado que o peso w de um avaliador é dado pela Equação 5.1, em que n_m é o número de vezes em que o avaliador votou com a maioria absoluta em atributos de perfil do mesmo tipo de i e n_t corresponde ao número de vezes em que se formou uma maioria absoluta em perguntas do mesmo tipo de i em que o avaliador participou. Entende-se que há maioria absoluta em uma votação quando uma das opções de voto obtém mais de 50% dos votos (NORRIS, 1997). Esse critério de pesos dos avaliadores visa reduzir a influência de avaliadores mal-intencionados que recorrentemente responde perguntas incorretamente.

$$w = \frac{n_{\mathrm{m}}}{n_{\mathrm{t}}} \tag{5.1}$$

Por fim, após executar as duas etapas iniciais, o valor de t_i foi calculado seguindo os critérios definidos na Seção 4.2.2. A Figura 25 mostra os níveis de confiabilidade obtidos para as três

amostras consideradas neste experimento. Constatou-se que 94% dos atributos de perfil da *Amostra Real* obtiveram t_i maior ou igual a 0,5, enquanto 99% dos atributos de perfil da *Amostra Falsa A* e 96% dos atributos de perfil da *Amostra Falsa B* obtiveram t_i menor que 0,5. Os atributos de perfil da *Amostra Falsa B* obtiveram t_i maiores que os atributos de perfil da *Amostra Falsa A*, entretanto são expressivamente menores que os t_i obtidos pelo atributos de perfil da *Amostra Real*.

Figura 25 – Níveis de confiabilidade dos atributos de perfil obtidos com o *MyFriends-Checker*



Fonte: Elaborado pelo autor

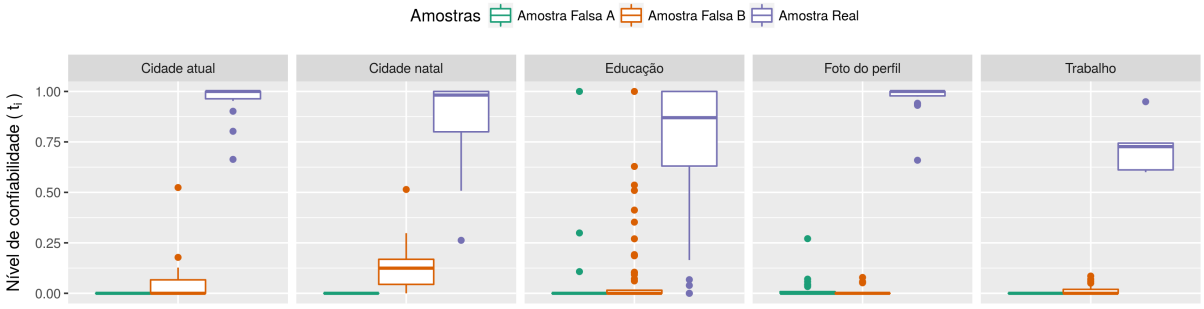
A Figura 26 apresenta diagrams *boxplot* com os resultados por tipo de atributo de perfil. Nota-se que para todos os tipos de atributo de perfil é possível definir um ponto de corte para distinguir os atributos de perfil da *Amostra Real* das demais amostras falsas.

Uma análise especial foi realizada em relação aos atributos de perfil do tipo trabalho *Estudante*, *Frases & Versos* e *Facebook* que foram identificados na Seção 5.2.2.2 como falso ou incorreto. Para isso os valores de t_i foram calculados para esses atributos, em que foi obtido os valores de t_i médio igual a 0,43, 0,31 e 0,42 para os atributos *Estudante*, *Frases & Versos* e *Facebook*, respectivamente. Esses valores obtidos para os atributos de perfil identificados como falso ou incorreto ficaram abaixo da média obtida pelos atributos de perfil do tipo trabalho da *Amostra Real*, que foi igual 0,73.

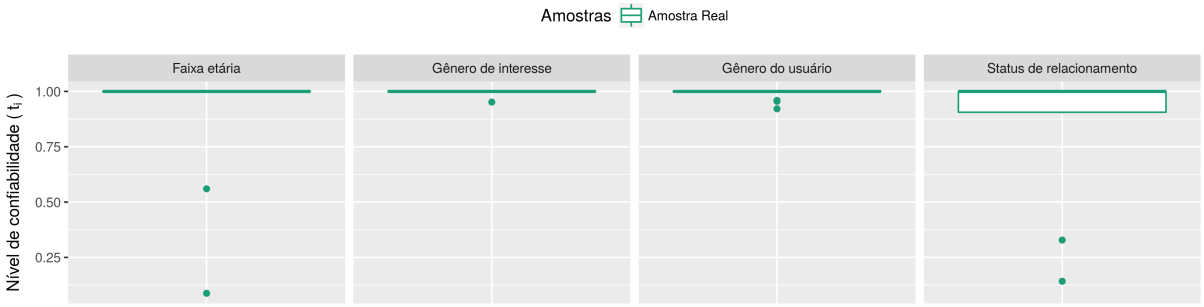
Os avaliadores no *MyFriends-Checker* possuem pesos que variam de zero até um. Esse dado pode ser interessante na aplicação do *framework*. A Figura 27 apresenta gráficos de dispersão correlacionando t_i com a soma dos pesos dos avaliadores que avaliaram um atributo i que compõe o perfil de um usuário. Em cada gráfico também é apresentada uma linha de regressão linear. Nota-se uma correlação indicando que quanto maior a soma dos pesos do avaliadores maior o t_i obtido na *Amostra Real*. O inverso é constatado para *Amostra Falsa A* e *Amostra Falsa B*. É visível que atributos de perfil das amostras falsas somente obtiveram t_i próximo a um quando a soma dos pesos dos avaliadores também está próximo de um. Com isso,

Figura 26 – Níveis de confiabilidade dos atributos de perfil obtidos com o *MyFriends-Checker* detalhados por tipo

(a) Atributos de perfil com opções de respostas dinâmicas



(b) Atributos de perfil com opções de respostas fixas



Fonte: Elaborado pelo autor

pode ser interessante incorporar filtros ao *framework* para definir um somatório mínimo de pesos dos avaliadores. Por exemplo, se considerarmos soma dos pesos dos avaliadores com o valor mínimo igual a 10, teríamos valor médio de t_i igual a 0,895 na *Amostra Real*, 0,007 na *Amostra Falsa A* e 0,059 na *Amostra Falsa B*. Quando se analisa os valores de médios de t_i sem considerar esse filtro obtemos 0,886 na *Amostra Real*, 0,012 na *Amostra Falsa A* e 0,068 na *Amostra Falsa B*.

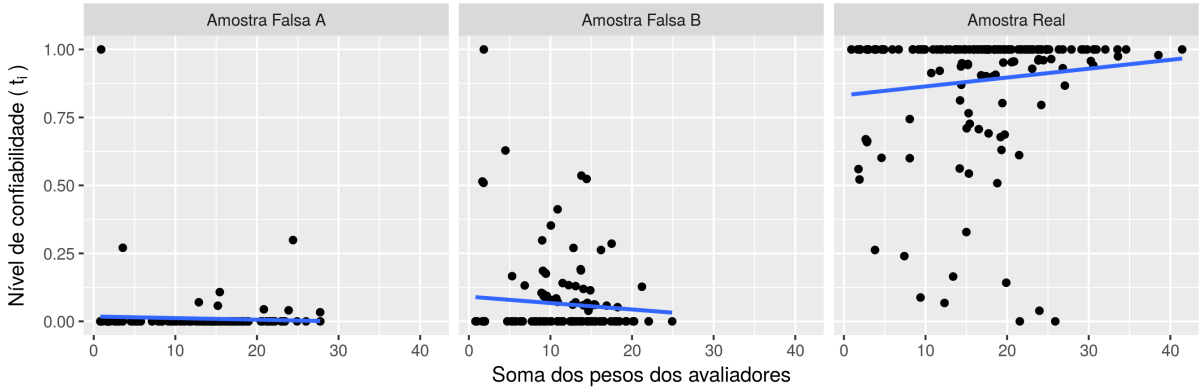


Figura 27 – Correlação dos níveis de confiabilidade dos atributos de perfil obtidos com o *MyFriends-Checker* e a soma dos pesos dos avaliadores

Fonte: Elaborado pelo autor

Os usuários considerados neste experimento possuíam atributos de perfil relativamente homogêneos e tinham em comum o contexto estudantil; isso pode ter criado viés que influenciou os resultados obtidos. A solução desta limitação para trabalhos futuros seria diversificar os usuários divulgando o *MyFriends-Quiz* em outras regiões e outros contextos sociais.

5.2.5 Análise da complexidade

Os custos de execução de cada uma das três etapas do *MyFriends-Checker* foram analisados. Na primeira etapa se seleciona quem serão os avaliadores de um dado atributo i que compõe o perfil do usuário u. Somente os amigos de u o podem avaliar, contudo, quem determina se um amigo de u está habilitado para ser um avaliador são os seus amigos indiretos mediante avaliações sobre tipo de relacionamento. Com isso, a ordem de complexidade é $O(a*b*k)$, em que a corresponde ao número de amigos de u, b corresponde ao número médio dos amigos indiretos de u e k corresponde ao número médio dos amigos indiretos dos amigos de u.

Na segunda etapa, para calcular os pesos dos avaliadores é necessário verificar o seu histórico de respostas e qual a opção formou maioria dentre as perguntas que o avaliador respondeu. Dessa maneira o custo de execução encontrado foi $O(e*q^2)$, em que e corresponde ao número de avaliadores e q é o número médio de perguntas respondidas pelos avaliadores.

A terceira e última etapa do *MyFriends-Checker* consiste no cálculo final para determinar o nível de confiabilidade de i. Esse cálculo consiste em verificar os pesos e as respostas dos avaliadores; portanto, o tempo de execução constatado é $O(e)$.

5.2.6 Comparação com o FaceTrust

A estrutura geral do *MyFriends-Checker* foi inspirada na proposta do FaceTrust (SIRIVIANOS et al., 2014), que consiste em uma solução de *crowdsourcing* que determina níveis de confiabilidade para cada atributo de perfil de um usuário de rede social *on-line* com base nos votos dos seus amigos. Entretanto, algumas fraquezas no FaceTrust foram identificadas e neste trabalho buscou-se aprimorar com o *MyFriends-Checker*.

A principal fraqueza constatada no FaceTrust é a previsibilidade da opção de resposta desejada pelo usuário avaliado. No FaceTrust as perguntas têm opções de respostas apenas binárias ('verdadeiro' ou 'falso'), sendo que a opção declarada pelo usuário avaliado é sempre a opção 'verdadeira'. No FaceTrust ainda é possível escolher quais amigos o podem avaliar e mesmo é possível convidar um amigo para o avaliar. No *MyFriends-Quiz*, *front-end* do *MyFriends-Checker*, um usuário pode ser avaliado por qualquer amigo e, ao iniciar o processo de avaliação, o avaliador é questionado sobre amigos aleatórios e possui tempo máximo de 20 segundos para responder, característica não observada no FaceTrust. O *MyFriends-Quiz* busca reduzir a previsibilidade da resposta correta ao sempre apresentar múltiplas opções de respostas.

O *MyFriends-Quiz* aplicou recursos de gamificação. No FaceTrust isso não foi constatado. Deve-se considerar que soluções *crowdsourcing* dependem do voluntarismo dos seus colaboradores para se obter êxito, portanto é importante adotar medidas que aumentem o engajamento e interesse dos participantes em avaliar seus amigos.

O FaceTrust incorpora técnica de detecção de *sybils* para determinar o peso dos avaliadores no processo de cálculo do nível de confiabilidade de um atributo de perfil. Na elaboração do *MyFriends-Checker* foi compreendido que detecção de *sybils* consiste em tarefa distinta da validação da identidade de usuário de rede social *on-line*. Portanto, decidiu-se propor um *framework* mais flexível que não ficasse engessado com nenhuma abordagem estranha ao seu objetivo principal. Ainda mais que nada impede que se apliquem paralelamente ao *MyFriends-Checker* soluções de deteção de *sybils*.

Em relação aos experimentos, o FaceTrust foi avaliado apenas com atributos dos tipos idade, profissão, localidade e sexo. Já o *MyFriends-Checker* foi experimentalmente avaliado considerando atributos dos tipos foto do perfil, gênero do usuário, faixa etária, cidade natal, cidade atual, histórico de estudo, histórico de trabalho, status de relacionamento e gênero de interesse.

6 CONCLUSÕES

A motivação para realização deste trabalho consistia em descobrir como validar atributos de perfil de usuários de rede social *on-line*. A revisão da literatura mostrou que há no estado da arte na área de detecção, combate e validação de usuários maliciosos de redes sociais *on-line* alguma variedade de abordagens para detecção de contas comprometidas, detecção de clones, detecção de *sybils* e validação de identidade. Entretanto, notou-se escassez de trabalhos que validem perfis de usuários na granularidade de atributos de perfil.

Desta forma, dois *frameworks* para validação de atributos de perfil de usuários de rede social *on-line* foram propostos e experimentalmente avaliados. O primeiro chamas-se *EgoNetwork-Checker* que utiliza abordagem baseada em grafo e visa determinar níveis de confiabilidade para os atributos de perfil por meio da verificação da coerência da *ego-network* do usuário com fenômenos comuns nas redes sociais. O outro *framework* considerado neste trabalho é referenciado por *MyFriends-Checker* que utiliza abordagem baseada em votação apoiada por *crowdsourcing* para atribuir níveis de confiabilidade aos atributos de perfil de usuários de rede social *on-line*. Este trabalho considerou duas abordagens distintas para resolver o mesmo problema com o intuito de analisar experimentalmente os resultados de cada uma das abordagens consideradas.

Para avaliar experimentalmente o *framework EgoNetwork-Checker* foi utilizada uma amostra real da rede social Google+. Também foi gerada sinteticamente uma amostra artificial para simular usuários com atributos de perfil falsos. Os resultados mostraram que em geral os atributos de perfil da amostra real obtiveram níveis de confiabilidade maiores que os atributos de perfil da amostra artificial. As amostras de dados continham atributos de perfil do tipo cidade, empresa, escola e profissão, sendo que os níveis de confiabilidade obtidos para os atributos de perfil do tipo empresa e escola permitiram melhor distinção entre atributos de perfil reais e falsos que os do tipo cidade e profissão.

No segundo experimento realizado neste trabalho, um jogo de perguntas e respostas entre usuários do Facebook denominado *MyFriends-Quiz* foi implementado para funcionar como o *front-end* do *MyFriends-Checker*. Por meio do *MyFriends-Quiz*, usuários avaliaram a veracidade dos atributos de perfil dos seus amigos. Os dados coletados e produzidos pelo *MyFriends-Quiz* serviram de insumos para análise experimental do *framework MyFriends-Checker*. *Ground truth* com base em atributos de perfil de 20 usuários honestos foi definido. Amostras com atributos de perfil falsos foram injetadas nos 20 usuários que compõem o *ground truth* do experimento a fim de se verificar se os amigos dos usuários avaliados reconhecem atributos de perfil falsos e verdadeiros. Os resultados mostraram que os atributos de perfil verdadeiros obtiveram níveis de confiabilidade expressivamente maiores que o atributos de perfil falsos.

Os resultados obtidos tanto no *EgoNetwork-Checker* quanto no *MyFriends-Checker* indicam que as premissas e abordagens consideradas na formulação desses *frameworks* contribuem para determinar níveis de confiabilidade dos atributos de perfil de usuários de rede social *on-line*. Não foi possível comparar estatisticamente os resultados desses dois *frameworks*, pois as amostras de dados consideradas não são as mesmas. Entretanto, conceitualmente foi possível constatar vantagens e desvantagens dos *frameworks* propostos neste trabalho. A exploração do conhecimento humano pelo *MyFriends-Checker* consiste no maior diferencial e também na maior barreira para implantação desse *framework*. Espera-se que o uso do conhecimento humano potencialize maior nível de acurácia, entretanto, engajar usuários de rede social para responder perguntas sobre seus amigos é um desafio considerável. A estrutura de um jogo, conforme foi experimentado por meio do *MyFriedns-Quiz*, deve ter sua eficácia avaliada ao longo do tempo, pois é comum jogos possuírem ciclo de vida caracterizado por grande audiência no momento do seu lançamento e algum tempo depois se tornarem desinteressantes. O *EgoNetwork-Checker* possui a vantagem de adotar abordagem automatizada, dispensando qualquer interação humana para produzir um resultado. Entretanto, os experimentos mostraram que para esse *framework* poder ser utilizado e obter melhores resultados é preciso que o usuário em avaliação possua um conjunto mínimo de amigos que tenham declarado o mesmo atributo de perfil. Isso resulta na reduçação do número de atributos de perfil passíveis de avaliação pelo *EgoNetwork-Checker*.

Como trabalho futuro pretende-se verificar se abordagens que contam com o *feedback* humano apresentam maior acurácia em relação a abordagens automatizadas. Outro trabalho futuro consiste em aperfeiçoar o *EgoNetwork-Checker* para considerar diferentes padrões de *ego-networks* e usuários. Em relação ao *MyFriends-Checker* deseja-se incorporar mecanismos de validação de resultados de *surveys* no sistema a fim de aprimorar a atribuição de pesos dos avaliadores. Também se deseja especificar um protocolo de autorização baseado no OAuth 2.0 que incorpore uma camada com *framework* de validação de atributos de perfil de usuários de rede social *on-line*. A ideia é que um sistema terceiro que utiliza dados autorizados por usuários de redes sociais *on-line* tenha informações da confiabilidade dos dados recebidos.

REFERÊNCIAS

AL-QURISHI, M. et al. Leveraging analysis of user behavior to identify malicious activities in large-scale social networks. IEEE Transactions on Industrial Informatics, IEEE, v. 14, n. 2, p. 799–813, 2018.

BAHRI, L.; CARMINATI, B.; FERRARI, E. Coip—continuous, operable, impartial, and privacy-aware identity validity estimation for osn profiles. ACM Transactions on the Web (TWEB), ACM, v. 10, n. 4, p. 23, 2016.

BAHRI, L.; CARMINATI, B.; FERRARI, E. Knowledge-based approaches for identity management in online social networks. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, Wiley Online Library, p. e1260, 2018.

BELLEFLAMME, P.; LAMBERT, T.; SCHWIENBACHER, A. Crowdfunding: Tapping the right crowd. Journal of business venturing, Elsevier, v. 29, n. 5, p. 585–609, 2014.

BHATTACHARYYA, P.; GARG, A.; WU, S. F. Analysis of user keyword similarity in online social networks. Social network analysis and mining, Springer, v. 1, n. 3, p. 143–158, 2011.

BIANCONI, G. et al. Triadic closure as a basic generating mechanism of communities in complex networks. Physical Review E, APS, v. 90, n. 4, p. 042806, 2014.

BLONDEL, V. D. et al. Fast unfolding of communities in large networks. Journal of statistical mechanics: theory and experiment, IOP Publishing, v. 2008, n. 10, p. P10008, 2008.

BOHACIK, J.; FUCHS, A.; BENEDIKOVIC, M. Detecting compromised accounts on the pokec online social network. In: IEEE. Information and Digital Technologies (IDT), 2017 International Conference on. [S.l.], 2017. p. 56–60.

BOSHMAF, Y. et al. Íntegro: Leveraging victim prediction for robust fake account detection in large scale osns. Computers & Security, Elsevier, v. 61, p. 142–168, 2016.

BOYD, D.; ELLISON, N. Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, v. 13(1), p. 210–230, 2007.

BRABHAM, D. C. Crowdsourcing as a model for problem solving: An introduction and cases. Convergence, Sage publications Sage UK: London, England, v. 14, n. 1, p. 75–90, 2008.

BRANDT, C.; LESKOVEC, J. Status and friendship: Mechanisms of social network evolution. In: Proceedings of the 23rd International Conference on World Wide Web. New York, NY, USA: ACM, 2014. (WWW '14 Companion), p. 229–230. ISBN 978-1-4503-2745-9. Disponível em: <http://doi.acm.org/10.1145/2567948.2577327>.

BREIMAN, L. Random forests. Machine learning, Springer, v. 45, n. 1, p. 5–32, 2001.

BRÓDKA, P.; SOBAS, M.; JOHNSON, H. Profile cloning detection in social networks. In: IEEE. Network Intelligence Conference (ENIC), 2014 European. [S.l.], 2014. p. 63–68.

CAETANO, J. A. C. et al. Utilizando análise de sentimentos para definição da homofilia política dos usuários do twitter durante a eleição presidencial americana de 2016. In: Congresso da Sociedade Brasileira de Computação-CSBC. [S.l.: s.n.], 2017.

CAO, Q. et al. Uncovering large groups of active malicious accounts in online social networks. In: ACM. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. [S.l.], 2014. p. 477–488.

CHOU, Y.-k. Actionable gamification: Beyond points, badges, and leaderboards. [S.l.]: Octalysis Group, 2015.

CURRARINI, S.; JACKSON, M. O.; PIN, P. An economic model of friendship: Homophily, minorities, and segregation. Econometrica, Wiley Online Library, v. 77, n. 4, p. 1003–1045, 2009.

DANEZIS, G.; MITTAL, P. Sybilinfer: Detecting sybil nodes using social networks. In: SAN DIEGO, CA. NDSS. [S.l.], 2009.

DAVIS, C. A. et al. Botornot: A system to evaluate social bots. In: INTERNATIONAL WORLD WIDE WEB CONFERENCES STEERING COMMITTEE. Proceedings of the 25th International Conference Companion on World Wide Web. [S.l.], 2016. p. 273–274.

DETERDING, S. et al. Gamification. using game-design elements in non-gaming contexts. In: ACM. CHI'11 extended abstracts on human factors in computing systems. [S.l.], 2011. p. 2425–2428.

DODDS, P. S.; MUHAMAD, R.; WATTS, D. J. An experimental study of search in global social networks. science, American Association for the Advancement of Science, v. 301, n. 5634, p. 827–829, 2003.

DOUCEUR, J. R. The sybil attack. In: SPRINGER. International Workshop on Peer-to-Peer Systems. [S.l.], 2002. p. 251–260.

EASLEY, D.; KLEINBERG, J. Networks, crowds, and markets: Reasoning about a highly connected world. [S.l.]: Cambridge University Press, 2010.

EGELE, M. et al. Towards detecting compromised accounts on social networks. IEEE Transactions on Dependable and Secure Computing, IEEE, n. 1, p. 1–1, 2017.

GAO, H. et al. Detecting and characterizing social spam campaigns. In: ACM. Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. [S.l.], 2010. p. 35–47.

GONG, N. Z.; FRANK, M.; MITTAL, P. Sybilbelief: A semi-supervised learning approach for structure-based sybil detection. IEEE Transactions on Information Forensics and Security, IEEE, v. 9, n. 6, p. 976–987, 2014.

GONG, N. Z. et al. Evolution of social-attribute networks: Measurements, modeling, and implications using google+. In: Proceedings of the 2012 ACM Conference on Internet Measurement Conference. New York, NY, USA: ACM, 2012. (IMC '12), p. 131–144. ISBN 978-1-4503-1705-4. Disponível em: <http://doi.acm.org/10.1145/2398776.2398792>.

HALBERSTAM, Y.; KNIGHT, B. Homophily, group size, and the diffusion of political information in social networks: Evidence from twitter. [S.l.], 2014.

HAMARI, J.; SJÖKLINT, M.; UKKONEN, A. The sharing economy: Why people participate in collaborative consumption. Journal of the Association for Information Science and Technology, Wiley Online Library, 2015.

HAN, X. et al. Alike people, alike interests? inferring interest similarity in online social networks. Decision Support Systems, Elsevier, v. 69, p. 92–106, 2015.

HAWLITSCHEK, F.; TEUBNER, T.; WEINHARDT, C. Trust in the sharing economy. Die Unternehmung, Nomos Verlagsgesellschaft mbH & Co. KG, v. 70, n. 1, p. 26–44, 2016.

HIMELBOIM, I. et al. Valence-based homophily on twitter: network analysis of emotions and political talk in the 2012 presidential election. new media & society, SAGE Publications, p. 1461444814555096, 2014.

HOWE, J. The rise of crowdsourcing. Wired magazine, v. 14, n. 6, p. 1–4, 2006.

HUANG, H. et al. Triadic closure pattern analysis and prediction in social networks. IEEE Transactions on Knowledge and Data Engineering, v. 27, n. 12, p. 3374–3389, Dec 2015. ISSN 1041-4347.

JIANG, M.; CUI, P.; FALOUTSOS, C. Suspicious behavior detection: Current trends and future directions. IEEE Intelligent Systems, IEEE, v. 31, n. 1, p. 31–39, 2016.

JIN, L.; TAKABI, H.; JOSHI, J. B. Towards active detection of identity clone attacks on online social networks. In: ACM. Proceedings of the first ACM conference on Data and application security and privacy. [S.l.], 2011. p. 27–38.

KERETNA, S.; HOSSNY, A.; CREIGHTON, D. Recognising user identity in twitter social networks via text mining. In: IEEE. Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference on. [S.l.], 2013. p. 3079–3082.

KHAYYAMBASHI, M. R.; RIZI, F. S. An approach for detecting profile cloning in online social networks. In: IEEE. E-Commerce in Developing Countries: With Focus on E-Security (ECDC), 2013 7th Intenational Conference on. [S.l.], 2013. p. 1–12.

KIRUTHIGA, S.; KANNAN, A. et al. Detecting cloning attack in social networks using classification and clustering techniques. In: IEEE. Recent Trends in Information Technology (ICRTIT), 2014 International Conference on. [S.l.], 2014. p. 1–6.

KOLL, D. et al. On the state of osn-based sybil defenses. In: CITESEER. Networking Conference, 2014 IFIP. [S.l.], 2014. p. 1–9.

KWAK, H. et al. What is twitter, a social network or a news media? In: ACM. Proceedings of the 19th international conference on World wide web. [S.l.], 2010. p. 591–600.

LALEH, N.; CARMINATI, B.; FERRARI, E. Graph based local risk estimation in large scale online social networks. In: IEEE. Smart City/SocialCom/SustainCom (SmartCity), 2015 IEEE International Conference on. [S.l.], 2015. p. 528–535.

LALEH, N.; CARMINATI, B.; FERRARI, E. Risk assessment in social networks based on user anomalous behaviour. IEEE Transactions on Dependable and Secure Computing, PP, n. 99, p. 1–1, 2017. ISSN 1545-5971.

LATOZA, T. D.; HOEK, A. van der. Crowdsourcing in software engineering: Models, motivations, and challenges. IEEE software, IEEE, v. 33, n. 1, p. 74–80, 2016.

LESKOVEC, J.; HORVITZ, E. Planetary-scale views on a large instant-messaging network. In: ACM. Proceedings of the 17th international conference on World Wide Web. [S.l.], 2008. p. 915–924.

LESKOVEC, J.; MCAULEY, J. J. Learning to discover social circles in ego networks. In: Advances in neural information processing systems. [S.l.: s.n.], 2012. p. 539–547.

LI, Y. et al. In a world that counts: Clustering and detecting fake social engagement at scale. In: INTERNATIONAL WORLD WIDE WEB CONFERENCES STEERING COMMITTEE. Proceedings of the 25th International Conference on World Wide Web. [S.l.], 2016. p. 111–120.

LIMA, H. S.; MARQUES-NETO, H. T. Utilizando métricas de ego-network para validação de atributos dos perfis de usuários de redes sociais on-line. In: Simpósio Brasileiro de Redes de Computadores (SBRC). [S.l.: s.n.], 2018. v. 36.

LIU, Y.-H. et al. Mining crowdsourcing photos for recognizing landmark areas. In: IEEE. Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2016 10th International Conference on. [S.l.], 2016. p. 12–19.

MCPHERSON, M.; SMITH-LOVIN, L.; COOK, J. M. Birds of a feather: Homophily in social networks. Annual review of sociology, JSTOR, p. 415–444, 2001.

MILGRAM, S. The small world problem. Psychology today, New York, v. 2, n. 1, p. 60–67, 1967.

MISLOVE, A. et al. You are who you know: inferring user profiles in online social networks. In: ACM. Proceedings of the third ACM international conference on Web search and data mining. [S.l.], 2010. p. 251–260.

MUKTA, M. S. H.; ALI, M. E.; MAHMUD, J. Identifying and validating personality traits-based homophilies for an egocentric network. Social Network Analysis and Mining, Springer, v. 6, n. 1, p. 74, 2016.

MULAMBA, D.; RAY, I.; RAY, I. Sybilradar: A graph-structure based framework for sybil detection in on-line social networks. In: SPRINGER. IFIP International Information Security and Privacy Conference. [S.l.], 2016. p. 179–193.

NEWMAN, M. E. Mixing patterns in networks. Physical Review E, APS, v. 67, n. 2, p. 026126, 2003.

NEWMAN, M. E. The structure and function of complex networks. SIAM review, SIAM, v. 45, n. 2, p. 167–256, 2003.

NORRIS, P. Choosing electoral systems: proportional, majoritarian and mixed systems. International political science review, Sage Publications for the International Political Science Association, v. 18, n. 3, p. 297–312, 1997.

OTTE, E.; ROUSSEAU, R. Social network analysis: a powerful strategy, also for the information sciences. Journal of information Science, Sage Publications Sage CA: Thousand Oaks, CA, v. 28, n. 6, p. 441–453, 2002.

PARRY, D. T.; TSAI, T.-C. Crowdsourcing techniques to create a fuzzy subset of snomed ct for semantic tagging of medical documents. Soft Computing, Springer, v. 16, n. 7, p. 1119–1127, 2012.

PELAEZ, J. I. et al. E-democracy e-government: Present and future. In: 2016 Third International Conference on eDemocracy eGovernment (ICEDEG). [S.l.: s.n.], 2016. p. 81–86.

RAMALINGAM, D.; CHINNAIAH, V. Fake profile detection techniques in large-scale online social networks: A comprehensive review. Computers & Electrical Engineering, Elsevier, v. 65, p. 165–177, 2018.

RAPOPORT, A. Spread of information through a population with socio-structural bias: I. assumption of transitivity. Bulletin of Mathematical Biology, Springer, v. 15, n. 4, p. 523–533, 1953.

RUAN, X. et al. Profiling online social behaviors for compromised account detection. IEEE Trans. Information Forensics and Security, v. 11, n. 1, p. 176–187, 2016.

SHAHABADKAR, R.; KAMATH, M.; SHAHABADKAR, K. R. Diagnosis of compromised accounts for online social performance profile network. In: IEEE. Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on. [S.l.], 2016. p. 1552–1557.

SHAN, Z. et al. Enhancing and identifying cloning attacks in online social networks. In: ACM. Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication. [S.l.], 2013. p. 59.

SILVA, L. A. d.; PERES, S. M.; BOSCARIOLI, C. Introdução à mineração de dados: com aplicações em R. [S.l.]: Elsevier, 2016.

SIRIVIANOS, M. et al. Leveraging social feedback to verify online identity claims. ACM Transactions on the Web (TWEB), ACM, v. 8, n. 2, p. 9, 2014.

SOLIMAN, A. et al. Diva: Decentralized identity validation for social networks. In: IEEE. Advances in Social Networks Analysis and Mining (ASONAM), 2015 IEEE/ACM International Conference on. [S.l.], 2015. p. 383–391.

SOLIMAN, A. et al. Cadiva: cooperative and adaptive decentralized identity validation model for social networks. Social Network Analysis and Mining, Springer, v. 6, n. 1, p. 1–22, 2016.

STEIN, T.; CHEN, E.; MANGLA, K. Facebook immune system. In: ACM. Proceedings of the 4th Workshop on Social Network Systems. [S.l.], 2011. p. 8.

TRAN, N. et al. Optimal sybil-resilient node admission control. In: 2011 Proceedings IEEE INFOCOM. [S.l.: s.n.], 2011. p. 3218–3226. ISSN 0743-166X.

VISWANATH, B. et al. An analysis of social network-based sybil defenses. SIGCOMM Comput. Commun. Rev., ACM, New York, NY, USA, v. 40, n. 4, p. 363–374, ago. 2010. ISSN 0146-4833. Disponível em: <http://doi.acm.org/10.1145/1851275.1851226>.

WANG, B.; ZHANG, L.; GONG, N. Z. Sybilscar: Sybil detection in online social networks via local rule based propagation. In: IEEE. INFOCOM 2017-IEEE Conference on Computer Communications, IEEE. [S.l.], 2017. p. 1–9.

WANG, G. et al. You are how you click: Clickstream analysis for sybil detection. In: Usenix Security. [S.l.: s.n.], 2013. v. 14.

WANG, G. et al. Social turing tests: Crowdsourcing sybil detection. arXiv preprint arXiv:1205.3856, 2012.

WANG, G. et al. Clickstream user behavior models. ACM Transactions on the Web (TWEB), ACM, v. 11, n. 4, p. 21, 2017.

WEI, W. et al. Sybildefender: A defense mechanism for sybil attacks in large social networks. IEEE Transactions on Parallel and Distributed Systems, v. 24, n. 12, p. 2492–2502, Dec 2013. ISSN 1045-9219.

WEN, J.; YUAN, Q. Social circles discovery based on structural and attribute similarities. In: 2016 IEEE Trustcom/BigDataSE/ISPA. [S.l.: s.n.], 2016. p. 1652–1659.

YADAV, N. M.; CHATUR, P. Compromised account detection and prevention by profiling social behavior and fass key concept. In: IEEE. Recent Trends in Electrical, Electronics and Computing Technologies (ICRTEECT), 2017 International Conference on. [S.l.], 2017. p. 164–168.

YANG, X.; CAO, Q.; SIRIVIANOS, M. SybilRank: Aiding the detection of fake accounts in large scale social online services. 2012.

YANG, Z. et al. Uncovering social network sybils in the wild. ACM Transactions on Knowledge Discovery from Data (TKDD), ACM, v. 8, n. 1, p. 2, 2014.

YU, H. et al. Sybillimit: A near-optimal social network defense against sybil attacks. IEEE/ACM Transactions on Networking, v. 18, n. 3, p. 885–898, June 2010. ISSN 1063-6692.

YU, H. et al. Sybilguard: Defending against sybil attacks via social networks. IEEE/ACM Transactions on Networking, v. 16, n. 3, p. 576–589, June 2008. ISSN 1063-6692.

ZHAI, Z. et al. Haiti earthquake photo tagging: Lessons on crowdsourcing in-depth image classifications. In: IEEE. Digital Information Management (ICDIM), 2012 Seventh International Conference on. [S.l.], 2012. p. 357–364.

ZICHERMANN, G.; CUNNINGHAM, C. Gamification by design: Implementing game mechanics in web and mobile apps. [S.l.]: "O'Reilly Media, Inc.", 2011.

APÊNDICE A -- QUESTIONÁRIO *MYFRIENDS-QUIZ*

Figura 28 – Questionário aplicado aos usuários do *MyFriends-Quiz*

Participação no MyFriends-Quiz

Prezado usuário do MyFriends-Quiz,
Este questionário integra uma pesquisa de cunho estritamente acadêmico que visa mapear como os usuários do MyFriends-Quiz utilizam o sistema e sua experiência.

* Required

1. **Email address** *

2. **Nome** *

3. **Como você respondia as perguntas?** *
Mark only one oval.
- ◯ Somente respondia as perguntas que tinha certeza
- ◯ Selecionava as respostas que pareciam mais óbvias, mesmo sem ter certeza
- ◯ Selecionava respostas de forma aleatória
- ◯ Selecionava intencionalmente as respostas erradas

4. **Os atributos de perfil que você declarou no Facebook são:** *
Mark only one oval.
- ◯ Completamente verdadeiros
- ◯ Parcialmente verdadeiros
- ◯ Completamente falso

5. **Quais pontos positivos do jogo?**

6. **Quais pontos negativos do jogo?**

Fonte: Próprio autor