Sistemas fuzzy complementam a detecção de socialbots por aprendizado de máquina

Carla C. Pacheco[a]*, Alex Garcia, Raphael Machado[b] e Ronaldo M. Salles[a]
[a]*Instituto Militar de Engenharia, Rio de Janeiro, Brasil.*
Praça General Tibúrcio, 80, 22290-270, Praia Vermelha
Rio de Janeiro, RJ, Brasil.
[b] *Instituto Nacional de Metrologia, Qualidade e Tecnologia, Diretoria de Metrologia Científica e Tecnologia*
Rua Santa Alexandrina, 416,
Rio de Janeiro, RJ, Brasil,
carlapacheco@globo.com

RESUMO: *A detecção de socialbots em Redes Sociais Online tem sido objeto de diversos estudos baseados em aprendizado de máquina. Este trabalho apresenta o uso de um comitê de classificadores para melhorar a acurácia da identificação de socialbots. O comitê associa o conhecimento obtido por algoritmos de aprendizado de máquina ao conhecimento heurístico humano, obtido por entrevistas e formalizado por regras fuzzy. Os resultados mostram que estas abordagens são complementares, uma vez que o uso conjunto destes algoritmos em um comitê apresenta uma acurácia acima de 93%, maior do que os mesmos algoritmos utilizados isoladamente.*

PALAVRAS-CHAVE: *Redes Sociais, Detecção de Socialbot, Aprendizado de Máquina, Lógica Fuzzy, Comitê de Classificação.*

ABSTRACT: *Machine learning has been widely used in the detection of socialbots in Online Social Networks. This paper presents the use of an algorithm committee to improve the accuracy of socialbots identification. The committee combines the knowledge obtained by machine learning algorithms and human heuristic knowledge obtained through interviews and formalized in fuzzy rules. Results show that these approaches are complementary, since their use in a single committee presents accuracy above 93%, better than each of the algorithms independently.*

KEYWORDS: *Social Networks, Detection of Socialbot, Machine Learning, Fuzzy Logic, Ensemble Learning*

1. Introdução

Problemas como influência em processos eleitorais e propagação de notícias falsas ganharam destaque recente nas mídias de comunicação. A detecção automática de *socialbots* é um caminho para resolver estes problemas. *Socialbots* são contas nas Redes Sociais *Online* (RSO) controladas automaticamente e projetadas para serem parecidas com usuários reais [1]. A existência destes robôs influenciou artigos e pesquisas em áreas como eleições ([2] e [3]), predições no mercado de ações [4] e a percepção da comunicação de agentes humanos e *socialbots* [5]. Este assunto é de importância fundamental para a segurança cibernética e, até mesmo, para a segurança nacional.

Em um relatório recente do Twitter [6], esta rede social afirma que pelo menos 5% de suas contas são totalmente automatizadas, ou seja, um número maior do que 16,5 milhões de contas no ano de 2017. Diversos trabalhos sobre detecção de *socialbots* utilizam algoritmos de aprendizado de máquina e, muitas vezes, do tipo supervisionado. Neste cenário, um dos requisitos que se faz necessário é a existência de uma base de dados com contas rotuladas como humano ou *socialbot*.

Ao iniciar os trabalhos de detecção de *socialbots* usando aprendizado de máquina os autores detectaram problemas de qualidade com as bases rotuladas disponíveis para pesquisa. Os problemas principais eram a dúvida sobre a correção da rotulação e a diversidade das contas presentes nas bases. Em [7], os autores apresentam uma discussão sobre a correção do processo de rotulação das contas e a diversidade de humanos e *socialbots* presentes nas bases existentes. Adicionalmente, apresentam uma metodologia para construção de bases de dados rotuladas com qualidade garantida. Esta metodologia foi usada para produzir uma base com postagens públicas no Twitter relacionadas às Olimpíadas Rio 2016, chamada de Base *Olympics*.

Outra vantagem da utilização da metodologia apresentada em [7], é a identificação dos melhores juízes que realizaram o processo de rotulação de contas [8]. Como continuidade do estudo desenvolvido no referido artigo, foi feita a identificação dos dois juízes mais bem avaliados que, então, foram escolhidos para a realização de entrevistas para a extração do seu conhecimento. Posteriormente este conhecimento foi formalizado na Lógica *Fuzzy* [9].

O Sistema Fuzzy resultante apresentou acurácia próxima a 85% para ambas as classes, humano e *socialbot*. O experimento foi realizado em uma base de dados balanceada, composta por 2500 contas, incluindo as da Base *Olympics* e as de outros trabalhos para contemplar *socialbots* de diversos tipos. Em seguida, este sistema foi agregado a um comitê composto por quatro algoritmos de aprendizado de máquina, cuja tomada de decisão escolhida foi o por voto por maioria. Foram escolhidos algoritmos de diferente natureza para compor o comitê: árvores de decisão, tabela de decisão, redes neurais e FURIA, além do algoritmo fuzzy com conhecimento humano obtido por entrevistas. O algoritmo FURIA também produz regras fuzzy, entretanto as regras representam conhecimento induzido a partir dos dados. O único sistema que trabalha com conhecimento heurístico humano foi o de regras fuzzy obtidas por entrevista.

Como resultado, este comitê de cinco algoritmos obteve um desempenho com acurácia próxima a 94%, superando cada membro do comitê individualmente e o comitê formado apenas pelos quatro outros algoritmos, comprovando que o Sistema Fuzzy contribuiu para a melhoria do desempenho final do comitê.

Este artigo está dividido da seguinte forma: na Seção 2, são apresentados os trabalhos relacionados; na Seção 3, está descrito o processo de construção da base de dados; a Seção 4 apresenta informações sobre a construção do sistema *fuzzy* para classificação das contas no Twitter; na Seção 5, são apresentados os resultados do comitê composto pelos algo-

ritmos de aprendizado de máquina e pelo Sistema Fuzzy; a Seção 6 conclui e apresenta os trabalhos futuros.

2. Trabalhos relacionados

Este trabalho inicia, apresentando outras pesquisas sobre a detecção de *socialbots* com a utilização de atributos quantitativos e aprendizado supervisionado. Benevenuto et al. [10] utilizaram o algoritmo SVM (descrito em [11]) que processou 23 atributos de usuário e 39 de *tweet*, resultando em aproximadamente 70% de acurácia para *socialbots* e em 96% para contas legítimas. Os autores apresentam uma discussão sobre o conjunto de atributos utilizado nos experimentos, argumentando que os menos significantes podem contribuir para o processo de classificação. A partir destes resultados, pode-se inferir que o modelo gerado por este algoritmo tende a classificar as contas como humanos.

Freitas et al. [12] basearam seu estudo no de Zhang e Paxson [13], porém consideraram mais atributos, divididos em três categorias: usuário, conteúdo e linguística. Freitas et al. utilizaram a base de dados de Cha et al. [14] e consideraram as contas com, no mínimo, 30 *tweets*, resultando em mais de 110 mil contas e quase 43 milhões de *tweets*. Foi utilizado o algoritmo *Random Forests* (descrito em [15]), com validação cruzada (CV) em 20 partições, que obteve resultados de 95% AUROC (Área sob a curva ROC).

De uma maneira diferente, Zhang e Paxson coletaram sua própria base composta pelo único atributo de *timestamp* de *tweets* públicos e, então, aplicaram o teste χ^2 de Pearson aos conjuntos de valores de minutos e de segundos com a finalidade de classificar as contas. Se o valor *p* retornado for alto, indica que os tweets são publicados com uma uniformidade não esperada de um humano. Os autores estimaram que 16% das contas ativas, na época, apresentaram alto grau de automatização, ou seja, eram de *socialbots*. Pode-se inferir que o *timestamp* do *tweet* parece ser um atributo importante a ser considerado na classificação de *socialbots*.

Lee et al. [16] consideraram contas com 200 ou mais *tweets* em uma base composta por mais de 5 milhões de *tweets* e 40 mil contas. Assim como em outros estudos, os classificadores baseados em árvores apresentaram os melhores resultados, especialmente o *Random Forests,* com mais de 98% de acurácia em conjunto de dados dividido em 10 partições com CV. Seguindo a mesma linha baseada em árvore de decisão, Cresci et al., em três de seus trabalhos [17], [18] e [19], procuraram detectar *fake followers*.

Em [18], foi empregado um classificador baseado em árvore de decisão. Os demais estudos ([17] e [19]) contaram com mais quatro bases de dados que foram consolidadas em uma única base balanceada com 3.900 contas e mais de 2,75 milhões de *tweets*. Estas contas pertenceram a *socialbots* e usuários legítimos em igual proporção. Novamente, o *Random Forests* apresentou o melhor desempenho com 99% de acurácia.

O trabalho de Ferrara et al. [20] indica o nível de atividade automatizada de uma conta, através da utilização de um conjunto de algoritmos que processa 1.150 características (detalhadas em Varol et al. [21]). Os autores alegam terem alcançado o resultado de 95% AUROC em uma base de Lee et al. [16], composta por mais de 30 mil contas. Este método de detecção é utilizado pela aplicação *web* "*Botometer*" [22], a qual foi testada por Haustein et al. [23] para classificar contas como *socialbots* e humanos. Os resultados destes testes mostraram que ambos os tipos de contas foram classificados incorretamente, onde os *socialbots* foram classificados como humanos, indicando uma tendência desta ferramenta a considerar qualquer conta como humano. À luz da constatação de Haustein et al., foram realizados testes nesta ferramenta com os *socialbots* listados em [24] e [25]. Novamente, quase todos foram classificados como humanos.

A ferramenta de Ferrara et al. foi utilizada para classificar uma base de dados composta por até 3 mil contas coletadas, no trabalho de Varol et al. [21]. O resultado da ferramenta foi de 89% AUROC, enquanto que a classificação manual alcançou apenas 86% de acurácia. O trabalho de Gilani et al. [26] também submeteu contas manualmente classificadas a esta mesma ferramenta e reportam baixa acurácia (entre 40% e 60%).

Nove algoritmos de aprendizado de máquina foram utilizados por Alarifi et al. [27] para classificar 3.020 contas manualmente rotuladas, em dois experimentos. O primeiro foi composto por duas classes (humano ou *socialbot*) e apresentou valores de acurácia compreendidos entre 80% e 91%. Já o segundo experimento considerou três classes (humano, *socialbot* ou híbrida) com valores de acurácia variando de 61% até 88%. Uma análise mais aprofundada dos trabalhos supracitados encontra-se em Pacheco [28].

Encontramos um único trabalho relacionado ao uso de lógica *fuzzy* para detecção de *socialbots*, Sadiq et al. [29], que utilizou lógica *fuzzy* e a comparou com outros classificadores, como o "*Botometer*", por exemplo. Vale ressaltar que este estudo, em particular, utilizou 3 mil contas de *socialbots* que foram compradas para comporem a base de dados de contas do Twitter. Esta abordagem para composição da base de dados pode ser considerada tendenciosa para a geração de modelos de detecção de *socialbots*, pois há uma prevalência de um mesmo tipo de *socialbot* na base.

3. Aquisição da base de dados

Foi utilizada uma nova base de dados no presente estudo, a Olympics, coletada no período pré-olímpico de 2016 (Pacheco [28]). A escolha do tema possibilitou que fossem trabalhados com novos atributos, dados atuais e tweets em múltiplos idiomas. Por ser uma base nova, foi possível aplicar a metodologia descrita em [7], que oferece garantia na qualidade da base de dados rotulada. Para coletar os dados de usuários e tweets, foi utilizada a API gratuita do Twitter [31] que contém uma série de limitações.

A metodologia [7] consiste em alguns passos, iniciando pela definição das opções de rótulos e de juízes que fazem a rotulação da base, que é dividida em subconjuntos para distribuição entre os juízes. Então, a concordância entre os juízes é avaliada para cada subconjunto rotulado. Caso um subconjunto apresente um valor inferior a um limite (escolhido pelo pesquisador), este subconjunto deve ser rotulado novamente por outros juízes ou, então, descartado. Para os subconjuntos com concordância satisfatória, são aproveitadas apenas as contas para as quais há concordância na rotulação. Ao final, é realizada a avaliação relativa dos juízes, atribuindo-lhes uma nota quantitativa.

Ao final do processo, foram coletadas 4.011 contas com perfil público. Após a filtragem de contas com 30 ou mais *tweets*, a base apresentou 3.825 contas para serem rotuladas. Os dados coletados compuseram uma base com mais de 10 milhões de *tweets*. Para processar e consolidar estes dados,

foram calculados e extraídos atributos estatísticos e de entropia. Alguns trabalhos relacionados utilizaram, analogamente, alguns destes atributos quantitativos, como [18], [19], [1], [10] e [21].

O processo de rotulação foi feito através da metodologia descrita em [7]. As contas foram divididas em 18 conjuntos com 200 contas e 1 conjunto com 225 contas. Cada conjunto foi rotulado por 2 juízes. A concordância entre os juízes foi avaliada usando o índice Kappa de Cohen. Três conjuntos que tiveram o índice inferior a 0,30 foram reclassificados para se enquadrarem no critério de qualidade. Foram atribuídas notas aos juízes de acordo com sua contribuição [7]. Os dois juízes do melhor conjunto rotulado obtiveram notas 0,416 e 0,280, respectivamente.

Uma vez identificados os melhores juízes, procurou-se extrair seu conhecimento por meio de entrevistas. As entrevistas foram conduzidas de maneira a permitir que os melhores juízes validassem o conhecimento prévio, contribuíssem com novos conhecimentos e elucidassem hipóteses e conhecimentos parciais. Desta forma, regras e conjuntos do Sistema Fuzzy puderam ser escritos e testados na base *Olympics* já rotulada. Por estas razões, a utilização da metodologia contribuiu em três frentes: a qualidade dos dados que serviram para treinamento dos algoritmos de aprendizado de máquina, a criação de novos atributos (em função de critérios mencionados na entrevista) e a composição de regras e conjuntos do Sistema Fuzzy.

4. Sistema fuzzy para detecção de socialbots

A metodologia utilizada permitiu a identificação dos melhores juízes, que foram entrevistados e seu conhecimento formalizado em regras que compuseram um Sistema Fuzzy para detecção de *socialbots*. O maior desafio no processo da construção do sistema *fuzzy* foi o de transpor o conhecimento dos juízes que é representado por termos linguísticos informais para valores escalares no sistema. Por isso, a condução da entrevista por uma pesquisadora experiente foi fundamental para o sucesso da construção do Sistema Fuzzy.

O Sistema Fuzzy foi implementado na linguagem Java com a biblioteca jFuzzyLogic [32] e foi projetado com 16 variáveis de entrada, 1 variável de saída e 28 regras. As regras mais simples, com apenas uma ou duas variáveis, foram as mais difíceis de serem identificadas, pois demandaram a consolidação de conhecimentos de várias fontes. O processo de composição das regras *fuzzy* incluiu abordagem empírica de observação e rotulação manual das contas, análise dos dados consolidados e extração do conhecimento dos juízes.

Apesar dos dois melhores juízes apresentarem um nível de concordância próximo a 100%, a entrevista realizada com ambos revelou que suas percepções sobre as contas foram diferentes. Estes pontos de vista distintos enriqueceram as entrevistas, contribuindo para a criação de regras complementares, que melhoraram a precisão do Sistema Fuzzy. Este processo é análogo ao processo cognitivo de tomada de decisão do ser humano.

Algumas opiniões de um juiz foram confirmadas pelo outro e isso facilitou o projeto das regras, como, por exemplo, a frequência de postagem de uma conta. Quando um usuário faz postagens intensivamente, é um indício de que se trata de um *socialbot*. Durante a codificação da regra, observou-se que a entropia do intervalo entre *tweets* é um indicador melhor do que o intervalo médio ou outras medidas estatísticas. Quando o valor da entropia do intervalo entre *tweets* está abaixo de um determinado limiar, a conta é considerada um "*socialbot*". Este é um típico exemplo de uma regra simples para inferência de um *socialbot*. As regras geradas e a definição dos atributos de entrada e saída encontram-se em Pacheco [28].

Outro exemplo é a razão entre a quantidade de seguidores de um usuário e a quantidade de contas que um usuário segue. Quando esta razão é muito alta ou baixa demais, a conta pode pertencer a um "*socialbot*". O critério de ser 'alto' é subjetivo e esclarecido, em parte, pela entrevista. O fato é que é extremamente difícil construir regras conclusivas. A combinação das regras é determinante para a classificação eficiente das contas. Para que isso aconteça, diversos aspectos devem ser analisados e mapeados.

Ao final do processo de geração do Sistema Fuzzy, foi realizado um teste com uma base de dados balanceada composta por 2.500 contas, com igual número de humanos e de *socialbots*, uma vez que a base *Olympics* é representativa e apresenta quantidades discrepantes de *humanos* e *socialbots*, o que pode gerar vieses em alguns algoritmos. Optamos por realizar o balanceamento desta base para contornar a raridade da classe *socialbot* e evitar tais tendências, adicionando *socialbots* e reduzindo a quantidade de *humanos*, escolhidos dentre os melhores conjuntos rotulados. Os dados da base balanceada foram obtidos de três fontes distintas: 1.250 *humanos* e 255 *socialbots* da base *Olympics*, 229 *socialbots* de Cresci et al. [19] e 766 *socialbots* de Lee et al. [16]. Desta maneira, a base rotulada (base *Olympics*) corresponde a 60% da base balanceada e todas as suas contas possuem 30 ou mais *tweets* coletados.

Tab1: Matriz de confusão com acurácia do Sistema Fuzzy na classificação da base balanceada

Humano	Socialbot	Classificado como	Acurácia
1.088	156	Humano	87,28%
162	1.094	Socialbot	

O total de acertos do Sistema Fuzzy foi de 2.182 contas, sendo 1.088 humanos e 1.094 *socialbots* corretamente classificados, conforme a matriz de confusão na Tabela 1. O percentual de acertos de *socialbots* superou o de humanos, o que mostra que o Sistema Fuzzy tende a classificar *socialbots* como "*socialbots*" e não como humanos, como é o caso de outras ferramentas já mencionadas.

5. Comitê de classificadores

Para estudar o uso do Sistema Fuzzy em conjunto com algoritmos de aprendizado de máquina, criamos um comitê de algoritmos para detecção de *socialbots*. Este comitê foi composto por quatro algoritmos de aprendizado de máquina e pelo Sistema Fuzzy apresentado na seção anterior.

Os quatro algoritmos de aprendizado de máquina escolhidos foram representantes de famílias distintas: *Random Forests* (RF), baseado em árvore de decisão [15]; *Decision Table* (DT) que constrói e utiliza um simples classificador de tabela de decisão [33]; Redes Neurais Artificiais (RNAs), com método de otimização BFGS para minimizar o erro da função de custo [34]; e o *Fuzzy Unordered Rule Induction Algorithm* (FURIA) proposto por Hühn e Hüllermeier [30] que aprende regras *fuzzy* a partir dos dados.

Tab 2: Matriz de confusão com acurácia dos algoritmos de aprendizado sobre a base balanceada

Algoritmo	Humano	Socialbot	Classificado	Acurácia
Random Forests	1.173	92	Humano	93,24%
	77	1.158	Socialbot	
Redes Neurais Artificiais	1.153	85	Humano	92,72%
	97	1.165	Socialbot	
Tabela de Decisão	1.153	117	Humano	91,44%
	97	1.133	Socialbot	
FURIA	1.189	106	Humano	93,32%
	61	1.144	Socialbot	

Estes algoritmos foram escolhidos porque ajudaram na análise dos atributos que compuseram o Sistema Fuzzy construído e são representantes de técnicas bem diferentes entre si. Os resultados da Tabela 2 mostram o desempenho individual de cada um dos algoritmos de aprendizado na base balanceada. Observamos que estes resultados são melhores do que o apresentado pelo Sistema Fuzzy (ver Tabela 1), onde o FURIA apresentou o melhor desempenho. Estes quatro algoritmos foram implementados no *framework* Weka [35] com seus parâmetros padrão.

Devido ao uso de validação cruzada levar um algoritmo a ter um desempenho maior quando comparado ao uso em conjuntos de treino e teste, optou-se por utilizar a segunda estratégia por ser a mais parecida com a utilização de um comitê de classificação de *socialbots* em um ambiente real. Para fins de avaliação do comportamento do comitê, todos os algoritmos utilizaram um conjunto de treino disjunto do conjunto de teste.

Para avaliar a contribuição positiva do Sistema Fuzzy ao comitê, foram testadas as seguintes variações do comitê:

Comitê Original: os quatro algoritmos de aprendizado junto com o Sistema Fuzzy.

Variação 1: apenas os quatro algoritmos de aprendizado de máquina (empates foram considerados *não-socialbots*, que, neste caso, são *humanos*), sem o Sistema Fuzzy.

Variação 2: os mesmos quatro algoritmos, onde o *FURIA* (algoritmo com melhor acurácia) passou a ter peso 2.

Tab 3: Matriz de confusão com acurácia de três versões do comitê na classificação da base balanceada

Comitê	Humano	Socialbot	Classificado como	Acurácia
Original	1.182	94	Humano	93,76%
	68	1.156	Socialbot	
Variação 1	1159	78	Humano	93,72%
	91	1.172	Socialbot	
Variação 2	1.179	94	Humano	93,64%
	71	1.156	Socialbot	

A matriz de confusão das três versões do comitê está na Tabela 3. A Tabela 4 apresenta outras métricas de desempenho dos comitês e dos algoritmos individuais, mostrando que o seu desempenho superou os 90% nas métricas de precisão, abrangência e F1 em testes preliminares com validação cruzada. Mesmo apresentando a menor acurácia entre os algoritmos usados, o Sistema Fuzzy contribuiu positivamente para o comitê, pois a acurácia do comitê original superou a acurácia das duas variações. Conjecturamos que a contribuição está relacionada ao fato do Sistema Fuzzy trabalhar com conhecimento humano formalizado, enquanto que os demais algoritmos trabalham com conhecimento obtido a partir dos dados (conhecimento induzido).

Tab4: Métricas dos algoritmos e comitês

Algoritmo / Comitê	Precisão	Abrangência	F1	Classe
Sistema Fuzzy	87,45%	87,04%	87,24%	Humano
	87,10%	87,52%	87,31%	Socialbot
DT	90,79%	92,24%	91,51%	Humano
	92,11%	90,64%	91,37%	Socialbot
RNAs	93,13%	92,24%	92,68%	Humano
	92,31%	93,20%	92,75%	Socialbot
RF	92,73%	93,84%	93,28%	Humano
	93,77%	92,64%	93,20%	Socialbot
FURIA	91,82%	95,12%	93,44%	Humano
	94,94%	91,52%	93,20%	Socialbot
C. Variação 2	92,62%	94,32%	93,46%	Humano
	94,21%	92,48%	93,34%	Socialbot
C. Variação 1	93,69%	92,72%	93,20%	Humano
	92,80%	93,76%	93,28%	Socialbot
C. Original	92,63%	94,56%	93,59%	Humano
	94,44%	92,48%	93,45%	Socialbot

6. Conclusões

O presente trabalho apresentou um comitê para detecção de *socialbots* composto por um Sistema Fuzzy e quatro algoritmos de aprendizado de máquina. Os experimentos foram realizados em uma base de dados composta por 2.500 contas do Twitter, onde metade pertencia a humanos e a outra, a diversos tipos de *socialbots*. Esta base foi rotulada através da metodologia descrita em [7], a qual garantiu a qualidade dos dados.

O Sistema Fuzzy foi desenvolvido a partir da obtenção do conhecimento dos melhores juízes que rotularam as contas. Este algoritmo foi o único a classificar de maneira equilibrada a quantidade de *socialbots* e de humanos, apresentando uma acurácia próxima a 87% para ambas as classes. A acurácia do comitê foi maior do que a de cada um dos algoritmos que o compõem. Além disso, a acurácia do comitê foi maior com o Sistema Fuzzy do que sem o mesmo. Sendo assim, foi comprovado que a utilização do Sistema Fuzzy auxiliou no processo de classificação de *socialbots*, melhorando os resultados do comitê. Pelas razões expostas, os sistemas *fuzzy* mostraram ser uma opção eficaz na detecção de *socialbots* aliados a outros algoritmos. A sua utilização neste contexto, assim como refinamentos em seus conjuntos, variáveis e regras, pode ser melhor explorada em trabalhos futuros.

Todos os algoritmos contaram com uma análise prévia para a realização da escolha dos atributos e de seus parâmetros. Desta forma, todas as etapas garantiram a robustez dos modelos gerados dos algoritmos e, consequentemente, do referido comitê. Neste último, melhorias poderiam ser feitas com a adição de outros algoritmos e a variação do processo de tomada de decisão.

As contribuições deste trabalho incluem: a aplicação da metodologia para construção de bases de dados rotuladas com qualidade garantida, proposta em [7], coletando uma nova base de dados com qualidade assegurada; o Sistema Fuzzy, a ser construído a partir de entrevistas com os melhores juízes; e o Comitê de classificadores, que inclui o Sistema

Fuzzy e algoritmos de aprendizado supervisionado.

Agradecimentos

Agradecemos ao apoio da CAPES, da FAPERJ e do CNPq. Também, agradecemos a Cresci et al. [19] e a Lee et al. [16] por terem cedido suas bases para estudo.

Referências Bibliográficas

[1] [1] Freitas, C. A. et al.; Reverse engineering socialbot infiltration strategies in Twitter. IEEE/ACM ASONAM, 2015.
[2] [2] Tumasjan, A. et al.; Predicting Elections with Twitter: What 140 Characters Reveal about Political Sentiment. AAAI ICWSM, Washington, DC, EUA, 2010.
[3] [3] Dickerson, J. P. et al.; Using sentiment to detect bots on twitter: Are humans more opinionated than bots? IEEE/ACM ASONAM, p. 620–627, 2014.
[4] [4] Bollen, J. et al.; Twitter mood predicts the stock market. Journal of Computational Science, Vol. 2, p. 1–8, 2011.
[5] [5] Edwards, C. et al.; Is that a bot running the social media feed? Testing the differences in perceptions of communication quality for a human agent and a bot agent on Twitter. Computers in Human Behavior, Vol. 33, p.372–376, 2014.
[6] [6] Mander, J. e McGrath, F.; GWI Social GlobalWebIndex's quarterly report on the latest trends in social networking,https://cdn2.hubspot.net/hubfs/304927/Downloads/GWI-Social-Summary-Q1-2017.pdf , acessado em agosto de 2018.
[7] [7] Pacheco, C. et al.; A Methodology for Constructing Labeled Data Sets for Socialbots Detection. Revista IEEE América Latina, submetido, 2017.
[8] [8] Pacheco, C. et al.; Building Reference Datasets to Support Socialbots Detection. Metrology for Industry 4.0 and IoT. IEEE, 2018.
[9] [9] Zadeh, L. A.; Fuzzy logic. Computer, Vol. 21, N. 4, p. 83–93, Abril, 1988.
[10] [10] Benevenuto, F. et al.; Detecting spammers on Twitter. Collaboration, electronic messaging, anti-abuse and spam conference (CEAS), Vol 6, p.12, 2010.
[11] [11] Joachims, T.; Text categorization with support vector machines: Learning with many relevant features. Nédellec C., Rouveirol C. (eds) Machine Learning: ECML. Lecture Notes in Computer Science, Vol 1398, Springer Berlin Heidelberg, 1998.
[12] [12] Freitas, C. et al.; Socialbots: Implicações na segurança e na credibilidade de serviços baseados no Twitter. SBRC, Santa Catarina, Brasil. p. 603–616, 2014.
[13] [13] Zhang, C. M. e Paxson, V.; Detecting and analyzing automated activity on twitter. Passive and Active Measurement, p.102–111. Springer, 2011.
[14] [14] Cha, M. et al.; Measuring User Influence in Twitter: The Million Follower Fallacy. AAAI ICWSM, Menlo Park, CA, EUA. AAAI Press. p.10-17, 2010.
[15] [15] Breiman, L.; Machine Learning (2001) 45: 5, Kluwer Academic Publisher, doi:10.1023/A:1010933404324
[16] [16] Lee, K. et al.; Seven Months with the Devils: A Long-Term Study of Content Polluters on Twitter. AAAI ICWSM, 2011.
[17] [17] Cresci, S. et al.; A Fake Follower Story: improving fake accounts detection on Twitter. IIT-CNR, Relatório Técnico TR-03, 2014.
[18] [18] Cresci, S. et al.; A Criticism to Society (As Seen by Twitter Analytics). IEEE International Conference on Distributed Computing Systems Workshops (2014), doi:10.1109/ICDCSW.2014.31.
[19] [19] Cresci, S. et al.; Fame for sale: Efficient detection of fake Twitter followers. Decision Support Systems, Vol. 80, p. 56–71, 2015.
[20] [20] Ferrara, E. et al.; The Rise of Social Bots. Communications of the ACM, 2016.
[21] [21] Varol, O. et al.; Online human-bot interactions: Detection, Estimation, and Characterization. AAAI ICWSM, 2017.
[22] [22] OSoMe project, CNetS, IUNI. Botometer. https://botometer.iuni.iu.edu/#!/, acessado em agosto de 2018.
[23] [23] Haustein, S. et al.; Tweets as impact indicators: Examining the implications of automated "bot" accounts on Twitter. Association for Information Science and Technology, 2015.
[24] [24] Wikipedia. Twitterbot; https://en.wikipedia.org/wiki/Twitter_bot, acessado em agosto de 2018.
[25] [25] Prime, M.; The best Twitter bots of 2015 – Quartz (2015); https://qz.com/572763/the-best-twitter-bots-of-2015/, acessado em agosto de 2018.
[26] [26] Gilani, Z. et al.; Of Bots and Humans (on Twitter). ASONAM IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, p. 349-354, 2017.
[27] [27] Alarifi, A. et al.; Twitter turing test: Identifying social machines. Information Sciences – Informatics and Computer Science, Intelligent Systems, Applications. Vol. 372, p. 332–346, 2016.
[28] [28] Pacheco, C. et al.; Detecção de Socialbots em Redes Sociais baseada em atributos quantitativos; Tese de Doutorado, Instituto Militar de Engenharia, Rio de Janeiro, Brasil, 2018.
[29] [29] Sadiq, S. et al.; Aafa: Associative affinity factor analysis for bot detection and stance classification in twitter. IEEE IRI (2017), doi:10.1109/IRI.2017.25.
[30] [30] Hühn, J. e Hüllermeier, E.; Furia: an algorithm for unordered fuzzy rule induction. Data Mining and Knowledge Discovery, Springer US. Vol 19, p. 293, 2009.
[31] [31] Twitter. GET statuses/user timeline — Twitter Developers, 2017. https://developer.twitter.com/en/docs/tweets/timelines/api-reference/get-statuses-user_timeline.html, acessado em agosto de 2018.
[32] [32] Cingolani, P. e Alcalá-Fdez, J.; jfuzzylogic: a robust and flexible fuzzy-logic inference system language implementation. IEEE International Conference on Fuzzy Systems, p. 1–8, 2012.
[33] [33] Kohavi, R.; The Power of Decision Tables. ECML, Creta, Grécia (1995). Springer-Verlag, p. 174–189, doi: 10.1007/3-540-59286-5_57.
[34] [34] Liu, D. C. e Nocedal, J.; On the Limited Memory BFGS Method for Large Scale Optimization. Mathematical Programming, Vol. 45, p.503, Springer-Verlag, 1989.
[35] [35] Frank, E. et al.; Data Mining: Practical Machine Learning Tools and Techniques, Morgan Kaufmann, Fourth Edition, 2016.