Identification of Fake Profiles in Twitter Social Network

Mário Antunes[1,2,3] **, Hugo Batista**[1]**, Baltazar Rodrigues**[1,4]

[1] School of Technology and Management, Polytechnic of Leiria, Portugal

[2] INESC-TEC, CRACS, University of Porto, Porto, Portugal

[3] Computer Science and Communication Research Centre, CIIC, Portugal

[4] Portuguese Judiciary Police (PJ), Portugal

mario.antunes@ipleiria.pt

Porto, Portugal, 18-22 October 2020

Mário Antunes

- PhD in Computer Science, University of Porto, Portugal
- Professor at Polytechnic of Leiria, Portugal
- Researcher at CIIC, Polytechnic of Leiria, Portugal
- Researcher at CRACS, INESC-TEC, Porto, Portugal

webpage: https://www.dcc.fc.up.pt/~mantunes
e-mail: mario.antunes@ipleiria.pt

Outline

- Motivation and goals
- Background
- Proposed methodology
- Dataset
- Preliminary results
- Conclusions and future work

Motivation and goals

- The widespread and intensive use of social networks
- Fake profiles promotes cybercrime and malicious activity
- Awareness on the use of fake profiles

So, we need to:

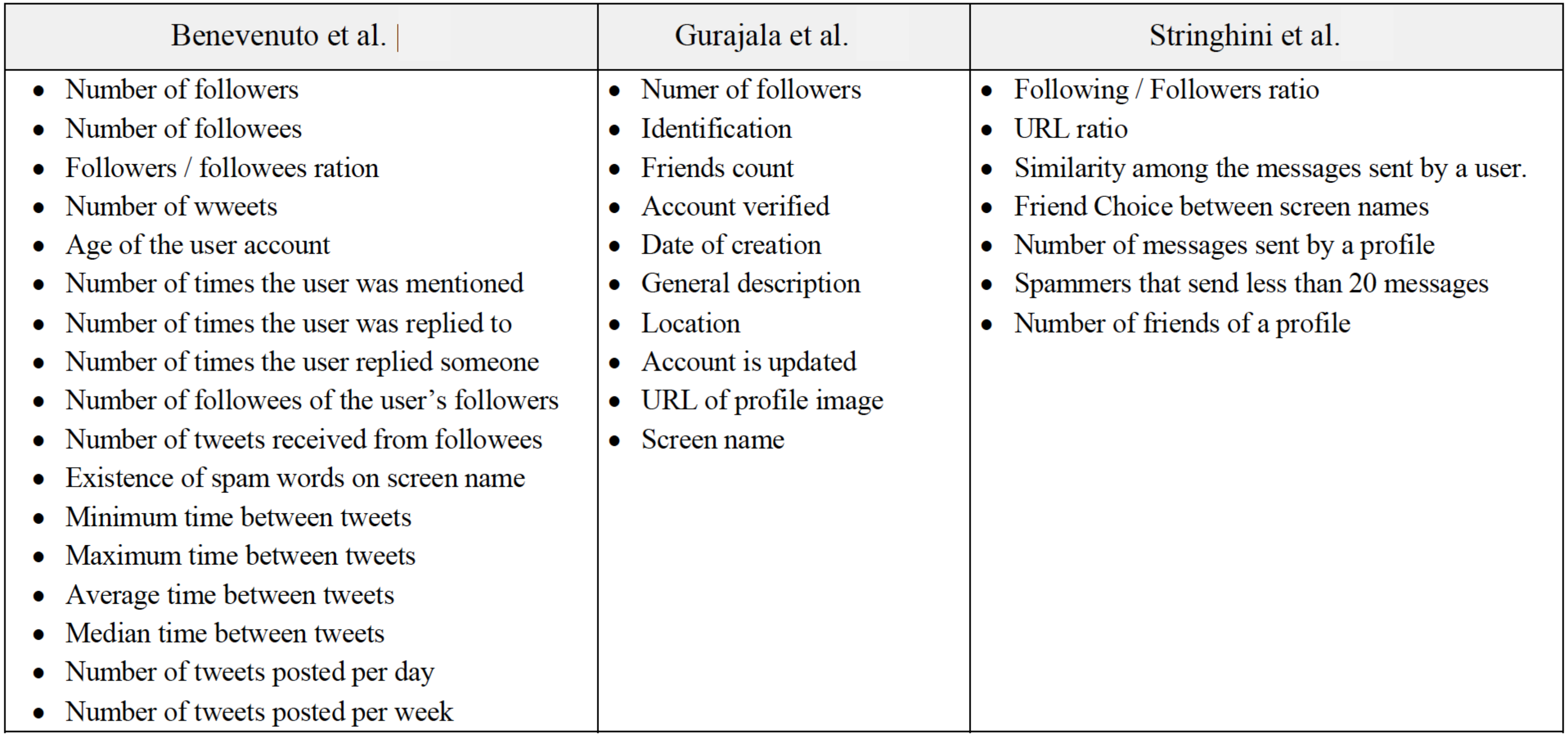
- To understand the meaning and use of fake profile
- To reinforce security in social networks

Previous research already the meaning of “fake profile”

Background

- Twitter uses short messages (280 characters) classified by a hashtag
- Each account has features (parameters) that may induce usage patterns

Background

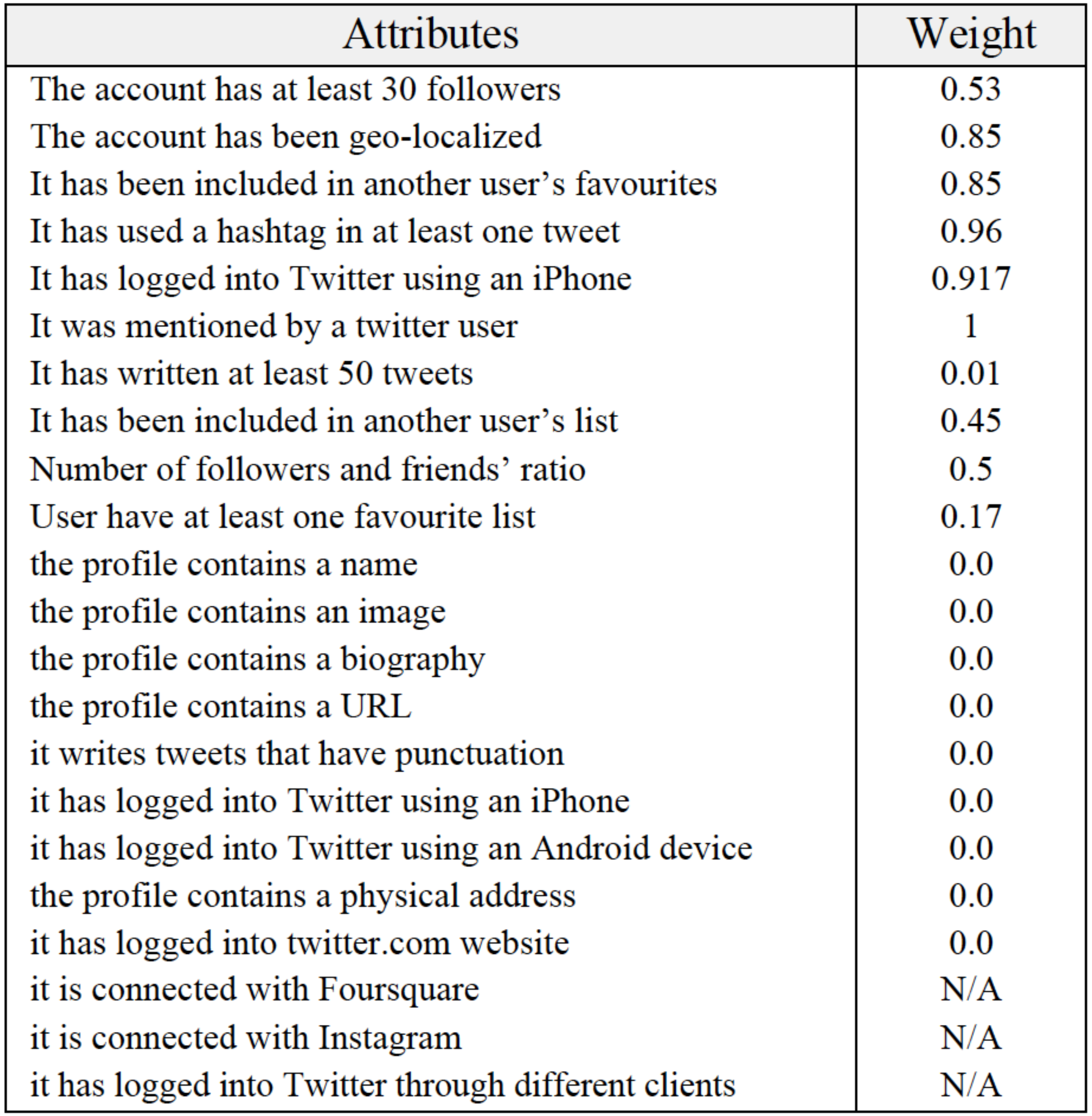


Benevenuto et al.	Gurajala et al.	Stringhini et al.
• Number of followers • Number of followees • Followers / followees ration • Number of wweets • Age of the user account • Number of times the user was mentioned • Number of times the user was replied to • Number of times the user replied someone • Number of followees of the user's followers • Number of tweets received from followees • Existence of spam words on screen name • Minimum time between tweets • Maximum time between tweets • Average time between tweets • Median time between tweets • Number of tweets posted per day • Number of tweets posted per week	• Numer of followers • Identification • Friends count • Account verified • Date of creation • General description • Location • Account is updated • URL of profile image • Screen name	• Following / Followers ratio • URL ratio • Similarity among the messages sent by a user. • Friend Choice between screen names • Number of messages sent by a profile • Spammers that send less than 20 messages • Number of friends of a profile

H. H. Ahmed El Azab, Amira M. Idrees, Mahmoud A. Mahmoud, "Fake Account Detection in Twitter Based on Minimum Weighted Feature set," Int. J. Comput. Inf. Eng., vol. 10, 2016

Background

- Initial parameters set
- 22 parameters

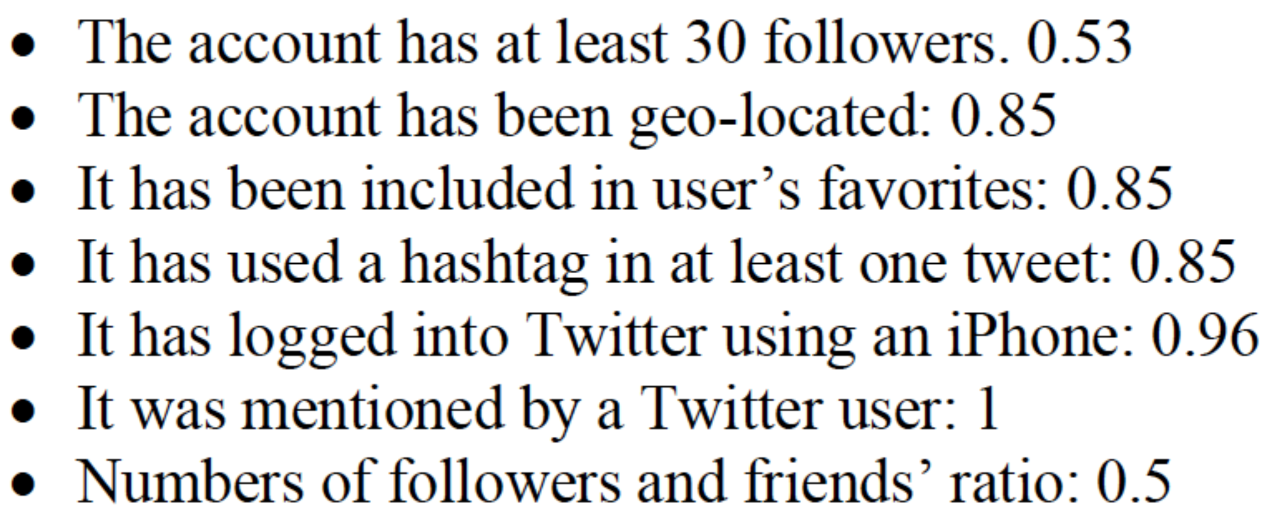


Attributes	Weight
The account has at least 30 followers	0.53
The account has been geo-localized	0.85
It has been included in another user's favourites	0.85
It has used a hashtag in at least one tweet	0.96
It has logged into Twitter using an iPhone	0.917
It was mentioned by a twitter user	1
It has written at least 50 tweets	0.01
It has been included in another user's list	0.45
Number of followers and friends' ratio	0.5
User have at least one favourite list	0.17
the profile contains a name	0.0
the profile contains an image	0.0
the profile contains a biography	0.0
the profile contains a URL	0.0
it writes tweets that have punctuation	0.0
it has logged into Twitter using an iPhone	0.0
it has logged into Twitter using an Android device	0.0
the profile contains a physical address	0.0
it has logged into twitter.com website	0.0
it is connected with Foursquare	N/A
it is connected with Instagram	N/A
it has logged into Twitter through different clients	N/A

H. H. Ahmed El Azab, Amira M. Idrees, Mahmoud A. Mahmoud, "Fake Account Detection in Twitter Based on Minimum Weighted Feature set," Int. J. Comput. Inf. Eng., vol. 10, 2016

Background

- The subset of 7 most relevant (>=50%)



- The account has at least 30 followers. 0.53
- The account has been geo-located: 0.85
- It has been included in user's favorites: 0.85
- It has used a hashtag in at least one tweet: 0.85
- It has logged into Twitter using an iPhone: 0.96
- It was mentioned by a Twitter user: 1
- Numbers of followers and friends' ratio: 0.5

H. H. Ahmed El Azab, Amira M. Idrees, Mahmoud A. Mahmoud, "Fake Account Detection in Twitter Based on Minimum Weighted Feature set," Int. J. Comput. Inf. Eng., vol. 10, 2016

Proposed method

1. To load a list of ”screen names”
2. Does the Twitter account exists and is active?
3. To retrieves parameters values through Twitter API
4. To calculates % of “fakeness”

Dataset

group name	Description	acc	tweets
genuine accounts (2011)	verified accounts that are human-operated	3,474	8,377,522
social spambots #1 (2012)	retweeters of an Italian political candidate	991	1,610,176
social spambots #2 (2014)	spammers of paid apps for mobile devices	3,457	428,542
social spambots #3 (2011)	spammers of products on sale at Amazon.com	464	1,418,626
traditional spambots #1 (2009)	training set of spammers used by C. Yang, R. Harkreader, and G. Gu.	1,000	145,094
traditional spambots #2 (2014)	spammers of scam URLs	100	74,957
traditional spambots #3 (2013)	automated accounts spamming job offers	433	5,794,931
traditional spambots #4 (2009)	another group of automated accounts spamming job offers	1,128	133,311
fake followers (2012)	simple accounts that inflate the number of followers of another account	3,351	196,027

100 examples of fake profiles

100 examples of legitime profiles

Results

- Mean values of fakeness probability (%)

	11 par	10 par	8 par	7 par
Genuine accounts	52,92	55,88	41,38	33,59
Fake accounts	87,73	86,50	83,13	80,71

Results

- Genuine accounts

%	>=40	>=50	>=60	>=70	>=80	>=90
11 par	96	66	41	24	15	9
10 par	70	45	29	22	15	9
8 par	64	41	29	19	11	7
7 par	45	29	20	19	10	7

Results

- Fake accounts

%	>=40	>=50	>=60	>=70	>=80	>=90
11 par	100	100	100	100	99	40
10 par	100	100	100	100	97	40
8 par	100	100	100	100	97	33
7 par	100	100	100	97	96	33

Conclusions

- Work in progress with promising preliminary results
- Decision support system for digital forensics
- Initial parameters set to calculate “*fakeness*” probability
- Future work:
  - To propose an updated version of the parameters vector
  - To test with additional Social Networks APIs
  - To make available a web-basedtool that may be widely used

Identification of Fake Profiles in Twitter Social Network

Mário Antunes[1,2,3] **, Hugo Batista**[1]**, Baltazar Rodrigues**[1,4]

[1] School of Technology and Management, Polytechnic of Leiria, Portugal

[2] INESC-TEC, CRACS, University of Porto, Porto, Portugal

[3] Computer Science and Communication Research Centre, CIIC, Portugal

[4] Portuguese Judiciary Police (PJ), Portugal

mario.antunes@ipleiria.pt

Porto, Portugal, 18-22 October 2020