Typification of Impersonated Accounts on Instagram

Koosha Zarei*, Reza Farahbakhsh*, Noël Crespi*

*Institut Mines-Télécom, Télécom SudParis, CNRS Lab UMR5157 Evry, France.

{Koosha.zarei, reza.farahbakhsh, noel.crespi}@telecom-sudparis.eu

Abstract—Fake accounts and Impersonators on Online Social Networks such as Instagram are turning difficulties for society. This has attended to an increasing interest in detecting fake profiles and investigating their behaviours. Questions like who are impersonators? what are their characteristics? and are they bots? will arise. To answer, we begin this research by collecting data from three important communities on Instagram including "Politician", "News agency", and "Sports star". Inside each community, four verified top accounts are picked. Based on the users who reacted to their published posts, we detect 4K impersonators [1]. Then we employed well-known clustering methods to distribute impersonators into separated clusters to observe obscure behaviours and unusual profile characteristics. We also studied the cross-group analysis of clusters inside each community to explore engagements. Finally, we conclude the study by providing a complete investigation of the bot-like cluster.

Index Terms—Impersonation; Bot Detection; Fake Profile; Instagram; Social Media; Unsupervised Clustering.

I. Introduction

One of the most widely used social media is Instagram. More and more of people, celebrities, sports players, politician, and organizations are signing up for profiles. Some have hundreds or thousands of followers spread across multiple profiles. The potential of social networks is often mistreated by malicious users who obtain individual information from genuine verified accounts. One of the most common ways of spreading fake news, disinformation, and false activities is the use of fake profiles, where malicious users present themselves in profiles impersonating fictitious or real persons. Impersonators are those accounts that are pretending to be someone we know or pretending to be or represent a company, brand or organisation.

In terms of criminal law, in the United State, criminal impersonation is a crime that is governed by states laws, which vary by state. It involved assuming a false identity with the intent to defraud another or pretending to be a representative of another person or organisation [2]. In this paper, with regards to Instagram as a growing Online Social Network, we are investigating to answer questions like who are the impersonators? in which community are more involved? Among impersonators, how many distinct hidden groups exist? what are their characteristics? and How impersonators are involved in terms of reactions?

To answer these questions, at first, we picked three distinct communities on Instagram such as "Politician", "News agency", and "Sports star". Inside each one, we selected four top verified genuine accounts and we collected a great number of posts beside comments and likes (in a seven-month period).

For each one, we detected and extracted the impersonator profiles and we ended up with 4K dataset. By using unsupervised clustering methods like K-Means and Spectral, we clustered them into three groups. The goal of clustering is to determine the internal grouping in a set of unlabelled data. Interestingly, each cluster represents the unique collection of users on Instagram with distinct profile characteristics and behaviour activities.

The main contributions of this study are:

- Identification of impersonators of top verified figures in three major communities on Instagram including "Politician", "News Agency", and "Sports Star".
- Perform an unsupervised clustering approach to find inner-groups of impersonators based on profile metrics.
- Provide a comparison of clusters in terms of profile characteristics and user behaviour activities to non-impersonator accounts.
- Cross category analysis of clusters to understand the distribution of activities and hidden actions.
- Provide a comprehensive study of the bot-like cluster to understand how they are operating on these communities.

The remaining of this study is as follows. Section II gives the related studies. The process of data crawling, the description of communities, and the dataset are described in section III. The methodology of identification of the impersonator is detailed in section IV. The full description of the unsupervised machine learning approach is in section V. Then, the characteristics of the clusters are compared in section VI. Additionally, the cross-group analysis of clusters among communities is presented in section VII and section VIII presents in detail analyse of the botlike cluster. Finally, section IX shows future directions and concludes the study.

II. Related work

Fake account: Recent research has worked on related research problems and dedicated a fair amount of work to study a different aspect of OSNs. In this era, looking to behavioural aspect of users and understand the different pattern of activities is still a hot topic of research. Several studies tried to shed light on this direction by profiling users based on their activities and reactions. This work [3] presents a novel technique to discriminate real accounts on social networks from fake ones. The writers from this [4] study provide a review of existing and state-of-the-art Sybil detection methods with an introductory approach and present some of the emerging open issues for Sybil detection in Online Social Networks.

TABLE I
DATASET CHARACTERISTICS AND COMMUNITIES

	Politician				News agency				Sports star			
	D. Trump	B. Obama	E. Macron	T. May	CNN	Fox	BBC	Reuters	L. Messi	C. Ronaldo	R. Nadal	R. Federer
#post	44	11	27	66	56	68	183	35	10	8	12	6
#comment	130K	175K	50K	20K	53K	90K	100K	79K	211K	196K	16K	22K
#like	3.9 M	5.08M	880K	520K	1.76M	1.60M	4M	1.9M	14.5M	14.27M	1.24M	6030K
crawled #profile [a]	500K	500K	500K	500K	500K	500K	500K	500K	500K	500K	500K	500K

[a] 500K randomly selected profiles from users who have reacted in the shape of Like and Comment.

Bot: On the other hand, the huge existence of Bots can alter the perception of social media influence, artificially enlarging the audience of some people, or they can impact the reputation of a company. The problem of rising social bots are discussed in [5]. There are various strategies to tackle the problem of bot detection. [6] suggested a profile-based approach and [7] proposed a novel framework on detecting spam content. Also, [8] presented a machine learning pipeline for detecting fake accounts and authors in [9], [10] present a method to classify bots and understand their behaviour in scale.

User Behaviour: On another line of research, the authors in [11] [12] look at the profile and behavioural patterns of a user and discussed existing challenges on different OSNs. By integrating semantic similarity and existing relationships between users, it is possible to match profiles across various OSNs [13] [14]. Also, [15] conducted a detailed investigation of user profiles and proposed a matching scheme. On Instagram, for the sake of mitigating impersonation attack, [16] explored fake behaviours and built an automated mechanism to detect fake activities.

As far as our knowledge, the problem of finding impersonators on Instagram and clustering the imposters is not studied in the literature and this is the first study that analyzed this phenomenon.

III. DATA COLLECTION

A. Crawling

For the purposes of data collection, with respect to Instagram API policies, we implemented an exclusive crawler in Python to receive data and store in a MongoDB server in the form of JSON files. In line with Instagram policies and user privacy and ethical consideration defined by the community, we only gather publicly available data that are only obtainable from Instagram. The whole data collection process is designed exclusively for research purposes and the data is stored in an anonymized format.

B. Communities

To investigate and understand the behaviour of impersonators and enhance the applicability of our model, it is essential to maintain the dataset to consists of data from a variety of categories. Toward that end, we extended the collection process into three separate influential communities including politician, news agencies and sports stars. As a result, we are dealing with a wide range of profile characteristics and user behaviours. In such a scenario, we have targeted the top

famous figures inside each community (Table I). All genuine accounts are official and are verified by Instagram.

- **Politician** community is of high interest. Having a large number of followers, fan pages, oppositions and supporters are the main reasons for selecting this community. Additionally, Political Bot is a new phenomenon in this area. Donald J. Trump (@*realdonaldtrump*) the president of the United States, Barack Obama (@*barackobama*) the previous president of the United States, Emmanuel Macron (@*emmanuelmacron*) the president of France, and Theresa May (@*theresamay*) the Prime Minister of the United Kingdom (all at the time of writing this paper) are included.

- **News Agency** is another vital community in which top English language news broadcasters including BBC (@*bbc*), CNN (@*cnn*), FoxNews (@*foxnews*), and Reuters (@*reuters*) are added. Use of Social Media is changing the relationship between the news agencies and the viewer. This community has a large number of audience from various groups.

- **Sports Star** community represents top sportsmen in football and tennis. Nowadays, thanks to social media, we see sporting star's habits, milestones and personal lives every day on our phones. Fake news, Fake profiles, and Disinformation are considered as serious difficulties inside this community. Leo Messi (@*leomessi*), Cristiano Ronaldo (@*cristiano*), Rafael Nadal (@*rafaelnadal*), and Roger Federer (@*rogerfederer*) are selected.

C. Dataset

In this study, we divided the genuine profile into three distinct communities as described in section III-B. We believe, while a wide diversity of audiences are included in these communities, we have chances to discover unusual sorts of impersonators such as political bots, sport fan pages, and spammers. Our primary target is to analyse posts published by genuine profiles and identify impersonators based on the reactions. The data collection process began in October 2018 and continued until April 2019. In the seven-month period, our specific-designed crawler was able to collect 550 posts, 1.3M comments, 20M likes, and 6M user profiles.

In Table I, *#post* shows total collected published post for each genuine profile inside its community. *T. May*, *BBC*, and *R. Nadal* have the most published posts in Politician, News agency, and Sports Star communities sequentially. *#comment* displays total number of comments issued in posts and *#like* reveals cumulative likes that are given to posts. Among users

who have reacted to the posts (in the shape of Comment and Like) we selected 500k profiles randomly (for each case) and crawled their information as it is displayed in "*crawled #profile*" row.

IV. IDENTIFICATION OF IMPERSONATORS

In our previous study [1], we provided a methodology to detect impersonator from non-impersonator and explained how to measure the profile similarity on Instagram. In the current study, we also used the same technique. The important profile features that are used are *username*, *display name*, *biography*, and *profile photo* which indicate the characteristics of the account. *least common metric* and *most common metric* are respectively the minimum and maximum value that a profile has a similarity in one or more of before-mentioned features. To extract impersonators, we need to detect users who have similar profile features compared to a genuine profile. Therefore, for measuring the likelihood of text-features, we utilized Term Frequency-Inverse Document Frequency (TF-IDF) transformation using NLTK and scikit-learn packages [17] [18]. Meanwhile, by employing a Convolutional Neural Network (CNN) learning method, we compared the similarity of the photos [1].

TABLE II
DISTRIBUTION OF IDENTIFIED IMPERSONATOR PROFILES OUT OF 500K ANALYZED USERS PER ACCOUNT

	Account	Detected Impersonator	avg. like per Impersonator	avg. comment per Imperso.
Politician	D. Trump	108	3.5	4.7
	B. Obama	38	2.8	3.0
	E. Macron	30	3.88	0.52
	T. May	17	1.22	0.50
News agency	CNN	12	1.3	1.9
	BBC	4	0.4	0.8
	Foxnews	16	1.42	2.14
	Reuters	18	4.5	0.25
Sports star	L. Messi	398	18.7	82.1
	C. Ronaldo	2589	164.2	374.6
	R. Nadal	189	22.9	7.5
	R. Federer	213	27.6	28.8

Table II summarise the number of detected impersonator among all use cases. Note that impersonators extracted out of 500k analysed users per account. In term of population, *D. Trump*, *Reuters,* and *C. Ronaldo* hold the largest detected impersonator among Politician, News agency, and Sports star communities, respectively. Additionally, *C. Ronaldo* has the highest number among all. *Avg. like* and *avg. comment* show the average number of like and issued comment by impersonators in each use case. *C. Ronaldo* has the largest number in both (among all).

V. WHO ARE IMPERSONATORS?

In this part, as the main purpose of this study, we believe that with respect to our three major communities, impersonators could have different motivations, aims, characteristics, and behaviours. So, the primary research questions are: among detected impersonators (see IV) how many potential meaningful clusters exist? Who are they? What are their characteristics? Accordingly, to discover these hidden inner

groups we will jump into using some well-known unsupervised clustering methods. In other words, this will give us insight into underlying patterns of different inner groups of impersonators.

A. Clustering

The first step to apply an unsupervised clustering is data collection (through the communities) which was described in III and the process of impersonation detection is fully explained in section IV. At this step, we have a nearly 4K dataset of impersonators from all communities (Table II) that can be used for clustering. Then, we picked the most important features of the impersonator dataset and at the final stage, we employed three famous clustering algorithms to arrange the clusters and compare the results (III).

The impersonator dataset contains normalised 10 features including *username similarity*, *name similarity*, *bio similarity*, *photo similarity*, *most common metrics (mcm)*, *number of followers*, *number of followees*, *number of media count*, *private status*, and *verified status*. To be able to visualise the dataset, the Principal Component Analysis (PCA) [19] procedure is applied to the data. Using the Principal Components the data is mapped into the new 2D feature space (Figure 1.b). Finally, K-means, Gaussian Mixture Model, and Spectral Clustering algorithms are applied to obtain clusters.

K-means is a clustering algorithm that returns the natural grouping of data points, based on their similarity and has been adapted to many problem domains. In order to estimate the optimal k (number of clusters) for using K-means, we used "Elbow" algorithm. It works by plotting the ascending values of k versus the total error obtained when using that k.
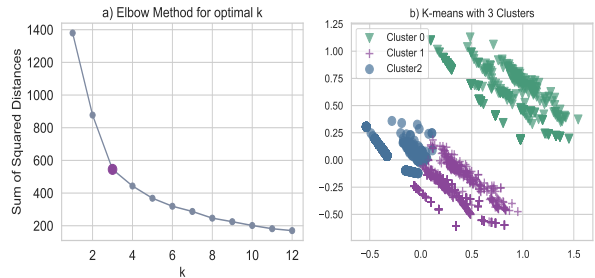

Fig. 1. Optimal k for K-means clustering (a) and PCA representation of data (b).

Generally, In Figure 1.a as k increases, the sum of squared distance tends to zero. It is obvious that as we add more clusters after 3 it doesn't give much better modelling on the data. As a result, the elbow is at k=3 indicating the optimal k for our dataset is 3. Next, we applied three popular clustering algorithms including K-means, Gaussian Mixture Model (GMM), and Spectral with parameters k=3 and random_state=100 for all case. PCA data representation with K-means clusters are depicted in Figure 1.b.

Table III illustrates the result of clustering. Interestingly, the results of all clustering methods are so close and all claim the same outcome. So in general, from impersonator dataset, we reached to three principal inner clusters that we are calling them *C0-Fan-Pages*, *C1-Ordinary-Users*, and *C2-BotLike*:

| Cluster | Population percentage | Similarity Percentage | | | | avg #mcm | Profile Characteristics | | | | Activity | Clusters'Given Lable |
		avg #username	avg #name	avg #bio	avg #photo		avg #follower	avg #followee	avg #private	avg #verified	avg #mediacount	
Cluster 0	50.33%	0.14	0.23	0.24	0.0	1.42	**13.3K**	737	**0.0**	0.01	124	Fan Page
Cluster 1	30.09%	0.09	0.12	0.29	0.03	1.25	**587**	**637**	**1.0**	0.0	77	Ordinary User
Cluster 2	19.57%	0.24	0.45	0.17	**1.0**	**2.85**	10.6K	491	0.09	0.0	**307**	Bot Like

[a] Most Common Metric: The maximum value that a profile has a similarity in one or more metrics (username, display name, bio, photo). Can be between 1 and 4.

- **C0-Fan-Pages** as we are dealing with different communities in this study C0-Fan-Pages could have different meanings. For example, in Politician, both supporting pages and opposition parties are considered as Fan Page. Normally they have similarity in #username, #name, and #bio features and all of them are public. The largest amount of #follower belongs to this group and they are publishing more than Ordinary Users.
- **C1-Ordinary-Users** group represents real users on Instagram that are expressing their feeling and showing their support of something or someone in biography. This can be done by putting a simple text, hashtag, or mention someone. So while there is a tiny similarity in *#name*, *#username* and *#photo*, but a big similarity can be seen in *biography*. Average *#mcm* is around 1 as there is similarity in just one metric. In comparison to other groups, the number of *#follower* is fewer, they are publishing less posts, and all are private accounts.
- **C2-BotLike** is the last and less populated cluster among all. Botlikes mimic the real accounts in most of the metrics. So, the average "most common metric" metric is almost 3. They have a great number of *#followers* and are so busy in terms of publishing post. Additionally, each Botlike has the exact or similar profile photo of the genuine account. These features indicate that Botlike might be a kind of Bot (section VIII).

From another viewpoint, in terms of the population, the considerable group is C0-Fan-Pages with more than 50% of the whole and C1-Ordinary-User and C2-Botlike with 30% and 19.57% respectively are in the second and third places. This shows a big representation of impersonated accounts acting as Fan of the genius account.

VI. ON ACTIVITY OF CLUSTERS

In this section, we aim to understand what are the major differences between the activity of each clusters? In other words, like differences in their profiles, do they have any distinctive behaviours? Toward that end, we consider *Comment*, *Like*, and *Post* features as user activities on Instagram. It is worth noting that the mentioned figures on this study comes only from the Comment and Like of users on the posts we have collected and reported in table I. In other hand, the figures about published Post (media count) shows the total published posts of users in their profile.

A. Media Count (Published Posts)

Added major activity feature which plays an important role in the identification of clusters is the media count or their own published post in their account. By looking at the profile of individual account inside each cluster, we can perceive how active they are (in terms of publishing). The average rate of publishing post from C2-Botlike cluster is 307 which is 2.5 times larger than C0-Fan-Page (124 posts), and 3.9 times greater than C1-Ordinary-User (77 posts). Differently to the other activity metric of this study (Like and Comment), this metric belongs to the users account and include all published posts of that users from the creation of the account. In other word, this is not limited to our dataset and the crawled posts.

TABLE IV
ACTIVITIES OF CLUSTERS IN OUR DATASET

Cluster	avg. #comment	avg. #like	avg. #mediacount
C0 - Fan Page	1.19	0.47	124
C1 - Ordinary User	1.56	0.48	77
C2 - Botlike	0.54	0.26	307

#comment and #like reported in this table represent the comments and likes generated in the crawled posts of this study.

B. Comments

The next step is to analyse issued comments by each cluster. Figure 2.a shows the cumulative distribution of the age of the comment published by each cluster in comparison to *non-impersonator* group which represent all the non-impersonator users. Generally, each cluster, in comparison to *non-impersonator*, are publishing comments with a higher rate. Within clusters, C0-Fan-Page has the greatest rate. In detail, while in the first hour, almost 20% of the total comments are issued by non-impersonator, the C0-Fane-Page and C1-Ordinary-User issued 40% of the comments. In hour 10, C0-Fan-Page and C1-Ordinary-User commented 20% and 10% more than non-impersonators, respectively. C2-Botlike has strange and unusual behaviour. It starts by issuing 20% (same as *non-impersonator*) and peaked at hour 10 (20% more than non-impersonator) and began to decrease.

Figure 2.b illustrates the same information with box plot representation (in minute). The median value of C0-Fan-Page and C1-Ordinary-User is close, but this number for C2-Botlike and non-impersonator is larger. Interestingly, the range of C2-Botlike is smaller than others indicating that it is commenting in a short period of time. In contrast, the biggest rang is for

C0-Fan-Page cluster. In this box plot, C0-Fan-Page and C1-Ordinary-User are commenting quicker.

In general, from Figure 2 we can observe that in terms of commenting, C0-Fan-Page and C1-Ordinary-User clusters are productive and they are issuing comments as soon as the post is published. Additionally, in C2-Botlike cluster, there is a strange and clear behaviour; botlikes began to comment from hour 1 and peaked (and stoped) at hour 10.
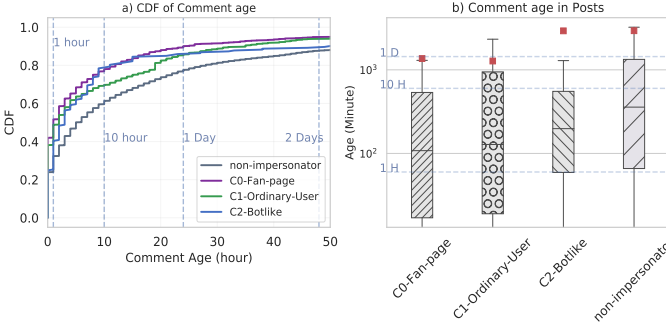
Fig. 2. Age of written Comments based on the timestamp of the corresponding post. Non-impersonator group represents normal accounts that are not detected as impersonators.

C. Like

Liking is another important metric which is surely valuable for understanding the activity of an impersonator. In global, Table IV presents the average rate of given like for all clusters. While C0-Fan-Page and C1-Ordinary-User clusters are so active in performing likes, in contrast, C2-Botlike is the laziest one (same pattern in comment). Interestingly, While C2-Botlikes published numerous posts (which is greater than others), but has a smaller number in both *average like* and *average comment*. Generally, we observe all clusters prefer to issue many comments while they do not have the same level of interest in giving like.

VII. CROSS CATEGORIES ANALYSIS

A. Distribution of cross activities

As the next step of this study, we desire to investigate what is the behaviour of clusters among categories. Toward that end, with respect to the population of clusters, we measured the distribution of individual cluster through three categories. To do so, we calculate the cumulative amount of reactions that are issued in each community, then we divided each by the number of unique users that are issuing them. So we achieve the distribution of impersonating accounts per communities. The result is shown in Figure 3.

In Figure 3.a the average written comments by users in clusters are presented. While C2-Botlikes are heavily interested in political communities (17 comments), but published fewer comments in Sports Star (with 3) and no comment in News agency. In contrast, C0-Fan-Page cluster is commenting equally (but fewer) in all three communities (almost 3). Among clusters, C1-Ordinary-User is the laziest one in terms of commenting (between 1 and 2). Figure 3.b shows the
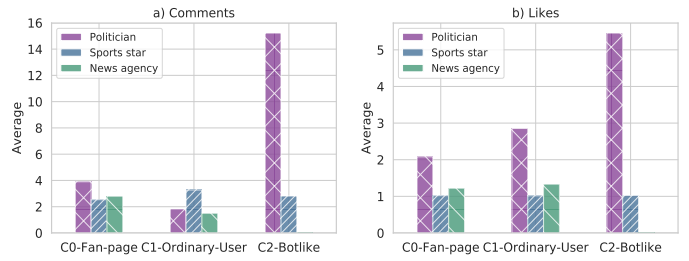
Fig. 3. Average cluster activities in all categories

average like given by impersonators of each cluster among categories. The C2-Botlike cluster is pretty active in liking political posts and is giving very fewer like to Sports star (with 1 like) and News agencies (no like). Also, It is interesting that all clusters are more into politician community. Both C0-Fan-Pages and C1-Ordinary-Users are almost giving the same rate of like to posts from News agencies and Sports star.

According to Figure 3, we witness several exciting findings. While C2-Botlikes are potentially interested in politics (as are giving a high rate of comments and likes), in contrast, they have no concern in News agencies at all. Also, on average the number of given comments is three times larger than the number of like. On the other side, C0-Fan-Pages preferred a little bit to post comments rather than giving likes in response to all communities.
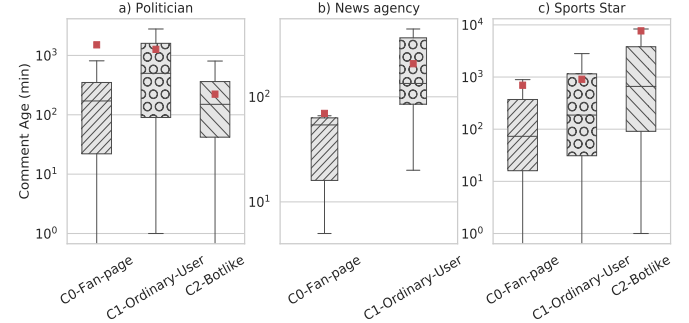
B. Diversity of comments

Fig. 4. Age of written Comments based on timestamp of the corresponding post across three categories

Let's analyse the age of comments in each cluster. Figure 4 is the box plot representation of the age of comments issued by each cluster across communities (in minute). With respect to the population of clusters, in Politician community, C0-Fan-Page is quicker, C1-Ordinary-User has a wider range, and C2-Botlike cluster has the smallest range. Amid the News agency community, C0-Botlike didn't post anything, C0-Fan-Page has the fastest react and the C1-Ordinary-User is the laziest. In the Sports Star community, C0-Fan-Page responded quicker following by C1-Ordinary-User and C2-Botlike clusters respectively.

Generally, in the News agency community, there is a significant difference between clusters. While C0-Fan-Page is so active in this community, but C2-Botlikes showed no interest.

VIII. Who are the Botlike cluster?

In this section, we intend to understand who are inside the C2-Botlike cluster? Are they definitely the representation of a bot cluster? Therefore, we began mining to obtain any particular patterns or bot activity.

TABLE V
DISTRIBUTION OF C2-BOTLIKE ACTIVITIES (LIKES AND COMMENTS ACROSS CATEGORIES)

Category	Account	Like		Comment		
		#botlike	portion of post Liked	#botlike	portion of post Commented	avg. #comment per post
Politician	D. Trump	13	15.9%	6	95.45%	2.2
	B. Obama	3	27.27%	0	0	0
	E. Macron	2	59.25%	2	14.81%	2
	T. May	6	71.27%	1	53.03%	1.02
Sports star	L. Messi	37	10%	4	90%	2.4
	C. Ronaldo	193	12.5%	17	100%	5.6
	R. Nadal	25	16.66%	6	50%	1.5
	R. Federer	12	16.6%	0	0	0

Table V explains the activity of C2-Botlike cluster in both reactions (Like and Comment) among all use cases. Interestingly, while C2-Botlike showed interest in Politician and Sports star communities, but there is no activity in the News agency community. It means in our dataset C2-Botlike impersonators have no curiosity in given like or comment to the news agencies. *#botlike* shows the number of detected C2-Botlike impersonator inside each reaction. It is crystal clear that the number of detected #botlike impersonator in Sports star (in both reactions) is greater than that number in the politician.

Among politician, *D. Trump* has the most botlike with 13 for like and 6 for comment reaction. in *B. Obama* case, #botlike prefer to give like (3) rather than publishing comments (0). Inside Sports star, while the *portion of post liked* from *R. Nadal* and *R. Federer* is the same (16%), but the population of #botlike for *R. Nadal* is double. Among all, *C. Ronaldo* has the highest detected #botlike in both reactions (193 and 17). Additionally, on average he received 5.6 comments in all his posts (100%).
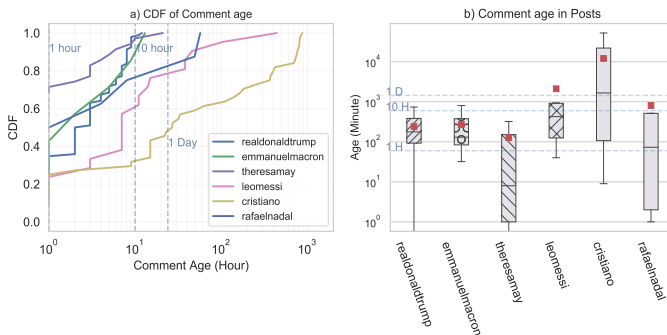

Fig. 5. Age of issued comments by C2-Botlike cluster.

To analyse deeper, Figure 5 gives us detailed information about comments issued by C2-Botlike. Plot 5.a is the CDF of the comment age in hour. In the first hour (important hour), *T. May* received around 70% of the total comments and took the first place. Following her, *R. Nadal*, *E. Macron*, and *D. Trump* caught nearly between 40% and 50%. Finally, *L. Messi* and *C. Ronaldo* collected 20%, fewer than others. Additionaly, by concidering the first 10 hours, while *T. May*, *D. Trump*, and *E. Macron* received all their comments, but others still collecting.

From another viewpoint, Figure 5.b is the Boxplot representation of the same data (in minute). The median, average point, and range of data for *D. Trump* and *E. Macron* is equal. *T. May*, *R. Nadal*, and *C. Ronaldo* have the greatest range among all, but *C. Ronaldo* is the laziest. As can be seen, while C2-Botlike reacted to the post of *R. Nadal* and *T. May* instantly, but they started to respond to others around the first hour.

Here is the analysis of C2-Botlike cluster:

- With *average mcm = 2.85*, they have the highest similarity in profile metrics among others (see V-A)
- 100% of them used similar profile photo (Table III)
- The rate of publishing by this cluster is nearly 3 times greater than others (see V-A).
- It has a pre-planned behaviour for publishing comment among communities. C2-Botlikes began to comment from hour 1 and peaked at hour 10 (see VI-B).
- While they have no interest in the News agencies, but showed a clear sign of matter in Politician (see VII-A).
- In general, the portion of giving likes is more than publishing comments by C2-Botlike (Table V).

In this study, we did not consider the text of comments and we performed the analysis just based on the profile activities and user behaviours. Regarding the findings in sections VII and VIII we perceive C2-Botlike cluster in both Politician and Sports star communities is the potential representation of the bots.

IX. Conclusion and Future Work

In conclusion, we did an investigation to discover impersonators in three leading communities on Instagram and apply different clustering methods to uncover who they really are. To our knowledge, this is the first paper that conducts such analysis on Instagram. We explained how impersonators are identified and how are used for further investigations. By using three clustering methods, we revealed how many hidden inner clusters exist and we provided a full analyse in terms of profile characteristics and user activities. Also, we provided the cross-category analysis to see the interests of each cluster in communities. Next, we moved one step further and analysed the bot-like cluster to recognise any suspicious behaviours that confirm they are bots. We considered profile characteristics, comments, likes, and age of reviews.

As future work, we planned to consider the text to understand what do they publish and see if there is any specific pattern inside. Considering Instagram Stories and IGTV could direct us towards new findings of fake activities. Another viewpoint is to study other social media and understand how impersonated are operating.

REFERENCES

[1] Koosha Zarei, Reza Farahbakhsh, and Noel Crespi. Deep dive on politician impersonating accounts in social media. In *2019 IEEE Symposium on Computers and Communications (ISCC) (IEEE ISCC 2019)*, Barcelona, Spain, June 2019.

[2] uslegal. https://definitions.uslegal.com/c/criminal-impersonation/, 2019.

[3] L. Caruccio, D. Desiato, and G. Polese. Fake account identification in social networks. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 5078–5085, Dec 2018.

[4] Devakunchari Ramalingam and Valliyammai Chinnaiah. Fake profile detection techniques in large-scale online social networks: A comprehensive review. *Computers Electrical Engineering*, 65:165 – 177, 2018.

[5] Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. The rise of social bots. *Commun. ACM*, 59(7), 2016.

[6] White J. S. Hudson B. Voter B. R. Matthews J. N. Gurajala, S. Profile characteristics of fake twitter accounts. 2016.

[7] S. Shehnepoor, M. Salehi, R. Farahbakhsh, and N. Crespi. Netspam: A network-based spam detection framework for reviews in online social media. *IEEE Transactions on Information Forensics and Security*, 12(7):1585–1595, July 2017.

[8] Cao Xiao, David Mandell Freeman, and Theodore Hwa. Detecting clusters of fake accounts in online social networks. In *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security*, AISec '15, pages 91–101. ACM, 2015.

[9] Zafar Gilani, Reza Farahbakhsh, Gareth Tyson, Liang Wang, and Jon Crowcroft. Of bots and humans (on twitter). In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*, ASONAM '17, pages 349–354, New York, NY, USA, 2017. ACM.

[10] Zafar Gilani, Reza Farahbakhsh, Gareth Tyson, and Jon Crowcroft. A large-scale behavioural analysis of bots and humans on twitter. *ACM Trans. Web*, 13(1):7:1–7:23, February 2019.

[11] Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera. Comparing twitter and facebook user behavior. *Comput. Hum. Behav.*, 52(C):87–95, November 2015.

[12] Bang Hui Lim, Dongyuan Lu, Tao Chen, and Min-Yen Kan. #mytweet via instagram: Exploring user behaviour across multiple social networks. IEEE/ACM ASONAM '15, pages 113–120. ACM, 2015.

[13] Ali Choumane, Zein Al Abidin Ibrahim, and Bilal Chebaro. Profiles matching in social networks based on semantic similarities and common relationships. In *Proceedings of the International Conference on Compute and Data Analysis*, ICCDA '17, pages 14–18. ACM, 2017.

[14] Katharina Krombholz, Dieter Merkl, and Edgar Weippl. Fake identities in social media: A case study on the sustainability of the facebook business model. *Journal of Service Science Research*, 4(2), Dec 2012.

[15] Oana Goga, Patrick Loiseau, Robin Sommer, Renata Teixeira, and Krishna P. Gummadi. On the reliability of profile matching across large online social networks. In *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '15, pages 1799–1808. ACM, 2015.

[16] Indira Sen, Anupama Aggarwal, Shiven Mian, Siddharth Singh, Ponnurangam Kumaraguru, and Anwitaman Datta. Worth its weight in likes: Towards detecting fake likes on instagram. In *Proceedings of the 10th ACM Conference on Web Science*, WebSci '18. ACM, 2018.

[17] Edward Loper Steven Bird, Ewan Klein. *Natural Language Processing with Python*. 2009.

[18] Fabian Pedregosa and Gaël et al. Varoquaux. Scikit-learn: Machine learning in python. *J. Mach. Learn. Res.*, 12:2825–2830, November 2011.

[19] I.T. Jolliffe. Principal component analysis. Springer, 2002.