Are There Bots even in FIFA World Cup 2018 Tweets?

Moath Bagarish
Dalhousie University
mbagarish@dal.ca

Riyad Alshammari
King Saud bin Abdulaziz University for Health Sciences
riyadalshammari@gmail.com

A. Nur Zincir-Heywood
Dalhousie University
zincir@cs.dal.ca

***Abstract*—Social media is an important communication medium in these days. Twitter is famous as microblogging service. It has been reported that social bots have been used in Twitter widely. In this research, we aim to understand whether bots are selective in the topics they participate or not. To this end, we explore tweets on FIFA World Cup. Our analysis indicate that there are bot activities even in tweets related to soccer (football) events but not just political topics.**

***Index Terms*—Service management, Tweet data analysis, Bot identification, Social media.**

I. Introduction

Social media has become the most popular way to communicate and socialize in this era. Twitter is one of the most famous social media services. Twitter allows users to share a tweet, which is a short text (up to 240 letters) that can be seen by a user's followers (or subscribers). Those tweets, if public, can be searched and viewed on the web by anyone using Twitter application or website. According to Twitter, it has around 330 million monthly active users in 2019 first quarter [1]. In 2014, Twitter reported that it has 500 million tweets per day[1].

It is estimated that 9% to 15% of Twitter active users are bots [2]. Social bots are softwares that programmed to automatically post social media messages and interact with humans [3]. These bots have various uses and effects on social media. For example, posting news and articles automatically from news sites, providing automatic response for company customers [4], and so on. However, many bots that are designed for malicious usage also appear recently. Their goals vary from spreading fake articles and news(misinformation) [5], spreading malware through suspicious websites [6], to malicious activities like promoting terrorist propaganda recruitment [7]. Their influence have been speculated to affect the outcome of even the U.S Presidential Election [8]. In short, such bot activities may decrease the credibility on the social media, might result in identity thefts or other cybersecurity and privacy problems [9]. Therefore, it is important to analyze such social media services of an organization to detect any bot activity and intention in order to be proactive against potential security and privacy issues.

In this paper, the objective is to explore the characteristics of bots participating in benign topics such as FIFA World Cup / Soccer Championships and to analyze how similar they might be to bots in other Twitter topics. In doing so, we aim to make the first step towards understanding some of the bot behaviours on social media and explore any potential indicators for these behaviours.

The rest of the paper is organized as follows. Section II summarizes previous research in this area. Section III introduces the dataset employed in this paper. Section IV presents the preliminary analysis of this dataset. Finally, conclusions are drawn and the future work is discussed in Section V.

II. Related Work

Understanding bot behaviour on social networks attracts the attention of both the cybersecurity and privacy researchers as well as the organizations. In the following we give a summary of the existing research in this area.

a) Bot threats: Some bots are designed for malicious and harmful activities. Since Twitter is mainly used for sharing news and information, some bots were designed to exploit this human weakness toward popular opinions. Aiello et al. show how bots can gain influence and popularity in social networks like Twitter [10]. They also showed that bots could widely be mistaken as humans. Echeverria and Zhou have discovered a large botnet on Twitter with a about 350K Twitter bot accounts [11]. These bots have shown evidence of being controlled centrally by a botmaster.

Moreover, bots can be used to control the flow and spread of information in Twitter for many purposes. In politics for example it can be used for political support as impersonating fake followers and number of retweets [12] in order to spread fake news to promote a party and demote the opponent [8] [13]. Bots are also used to spread malware [14].

The aforementioned threats and interactions are shown to affect the activities on social networks. Moreover, they have another negative side effect. Researchers have used social media data for different objectives. For example, studying social interactions, or degrees of freedom between users or organizations. Thus, in those analysis, the existence of malicious and spam bots may have a negative impact on the results that could be obtained. Additionally,

[1] https://blog.twitter.com/official/en_us/a/2014/the-2014-yearontwitter.html

978-3-903176-24-9 © 2019 IFIP

Twitter streaming API, which most researchers collect data from, is shown to be vulnerable to attacks so that the sample is not truly random [15].

b) Bot detection: One of the earliest works on bot detection in Twitter was published by Chu et al. They have classified Twitter accounts into three categories; (1) Humans, (2) Bots, and(3) Cyborgs, which are semi-human / semi-bot accounts. They used a combination of behaviour, and content related properties to build their classification system [16]. Their data was collected in 2009. Most of early bots were designed for simple tasks like regular posting of news, weather, or retweet a specific account. However, bots have evolved so that differentiating them from humans is a challenging task [3]. Many of these bots adopt an intelligent system to gain influence and deceive other users.

Varol et al. have studied the tweet and user features and examined how each contributes in identifying bots. They also propose a set of features that can improve the classification of bots [17]. Davis et al. have released a free online tool called "bot or not" and later called "botometer" this tool uses a classification framework to measure if a given account is a bot or human account in six measuring categories [18]. This tool uses the features proposed by [17]. The tool has been improved by the work presented by Varol et al. [2]. Yang et al. have studied people's interaction and feedback with this tool [19].

The work presented in the literature has achieved good accuracy in identifying bots. However, bots are becoming more sophisticated and intelligent. So, the task is still challenging. For this paper, we explore initial indications of bots in the FIFA World Cup tweets dataset we collected using the previous literature contributions.

III. Background and Methodology

In this section, Twitter API that is used to collect data and the overview of the data collection process are presented.

A. Twitter API

In order to analyze the tweets of the FIFA Wrold Cup, we employed Twitter API with Tweepy library to capture data. Twitter provides multiple APIs for developers to search historical tweets or to get the twitter live stream of public tweets. There are three types of streams: (1) Firehose stream -This is the full stream of public tweets; (2) Decahose stream -This is a 10% sample of firehose stream; and (3) The sample stream -This is about 1% of the firehose stream tweets and it is the only one out of three that is free of charge. Twitter also provides filtered stream which is the firehose stream that is filtered by hashtags or keywords and the user gets a volume less than or equal to 1% of firehose stream for free. Tweepy[2] is a library that provides an interface to all Twitter API functions using python. Tweepy maintains the conncetion and helps to identify errors related to using Twitter API.

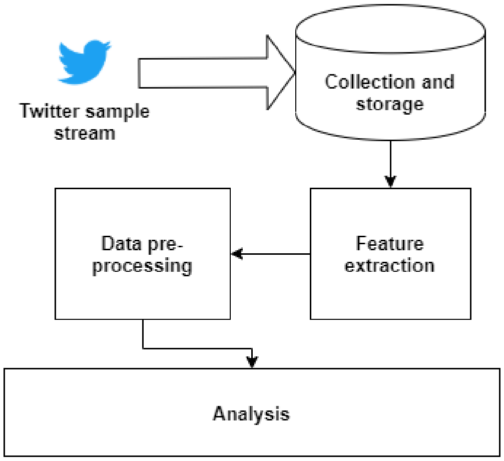

Figure 1: Overview of the steps followed

B. Data Collection

In this research, tweets were collected using the sample stream over the period that is started 24 hours before the opening match of FIFA world cup 2018 until 24 hours after the end of the final match. Since choosing a keyword is a difficult task because of different languages and different spelling in every language, tweets are filtered based on the research objectives and tasks performed. The collected tweets are approximately 470 GB in total. Figure 1 shows the steps followed to collect and pre-process the data.

C. Feature Extraction

Twitter sends each tweet as a tweet JSON object [20]. In this tweet object, there is over 50 data fields. Some of these fields are text related fields, user related feilds and other fields related to statistics of a given tweet. Since Twitter provides a lot of information for each tweet, there was a need to extract the necessary features for analysis. The source of tweet, for exampe, is in HTML format so it needs to be parsed and extracted. Another feature is the location of user, Twitter allows any text user input in this field so it has a lot of noise and non-location entries. The user country feature is extracted from the user profile information using a simple matching algorithm. The algorithm matches names of populated areas and cities and converts the matched information into country names. Another feature in the tweet object is *retweeted_status*. This feature have a nested tweet object if the current tweet is a retweet and empty otherwise.

IV. Analysis

The data collection started on June 15th, 2018. Unfortunately, due to the power outages and the technical problems it caused on the servers on our campus , we lost seven days of data collection (from June 27 to July 4th).Thus, the total number of tweets collected is 82 million unique tweets by 24.8 million users. The data we

[2] https://www.tweepy.org/

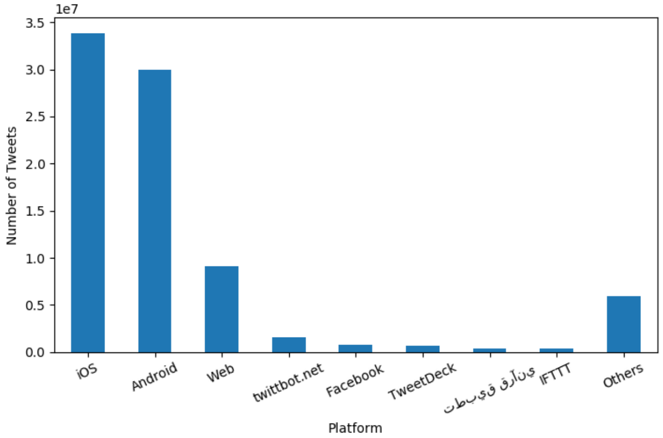

Figure 2: Number of tweets per platform.

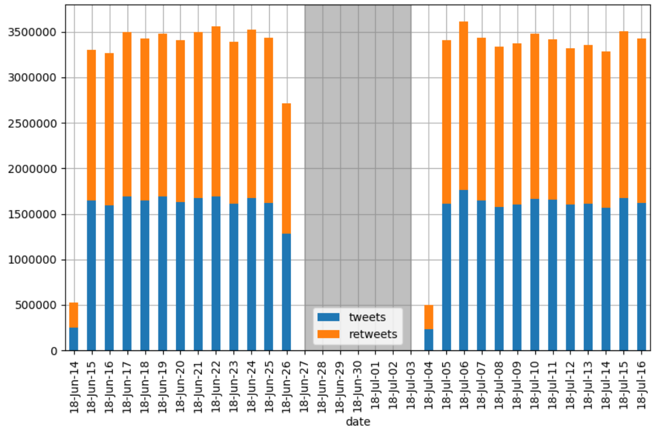

Figure 3: Number of tweets and retweets.

collected was not filtered by any keywords so it represents the 1% limit of randomly selected tweets that Twitter provides for free.

A. Client Source of Tweet

Twitter API provides registered third-party applications the ability to use most of the Twitter features. If a user wants to use any third-party application, they have to give that application permission to use his/her account. If the user has used that application to tweet, for example, the source of tweet field will have the registered information of the application used. The information in the source field is the name of the application and the URL of that application. Twitter only requires a unique application name for the application registration. In our data, the number of different applications used to tweet are approximately 127K.

Figure 2 shows a histogram for the different platforms used for tweeting in the data set analyzed in this paper. It is clear that more than 75% of the tweets were tweeted using handheld devices (mobile phones or tablets). Compared to a similar platform analysis done on NHL tweet data (collected in 2015 [21]), the percentage of mobile devices seems to be slightly lower in our dataset on FIFA World Cup. However, there is a slight increase in terms of other platforms in our dataset as well as different platforms only seen in our data set. It should be noted here that around 14,600 of those other platforms have the word ”bot” in their name.

B. Type of Tweets

Retweet is how a user shares a tweet of interest so those who follow his/her account can see the original tweeted message. During the days that tweets were collected, Figure 3 shows that retweets represent about 50% of total tweets per day. Number of retweets of a message can be considered as a measure of popularity of that message. According to Shao et al. [22], the spread of low credibility content on Twitter is usually started by bots at the first stage even though most of the work is continued by misinformed human users. Gorodnichenko et al. concluded that social bots can spread and boost mis-information [8]. In our collected data, most of the retweets happens within 24 hours of the original tweet while 27% are retweeted within 1 hour as shown in Figure 4. This behaviour can be used for analyzing and detecting bots behaviour.

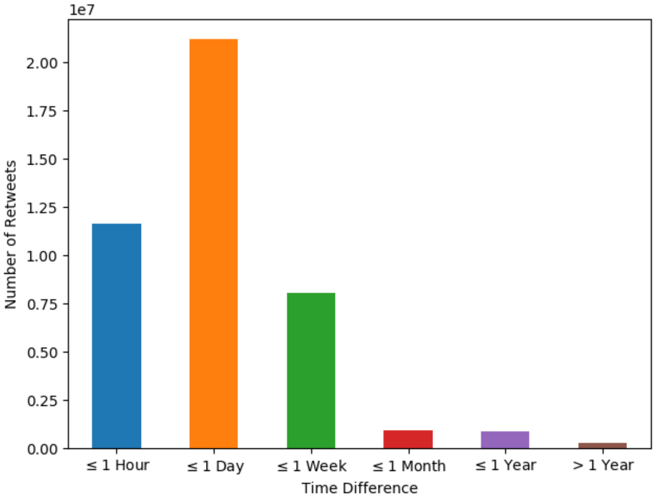

Figure 4: Time difference between retweet and the original tweet with frequency of retweets.

C. Location of Tweeters

About 20% of Twitter active users tweets from USA [3]. According to the collected data, 62% of the users does not share any type of location information. Most of the remaining 38% have location information text as part of the user profile and only 2.7% share their location coordinates in some of their tweets. We used quadrat counting method described in [23] to draw Figure 5. In this figure, the red dots show the different locations of participating Twitter accounts in our data set. The map shows the existence of tweets with coordinates in non-inhabitant areas like deserts, frozen lands, and oceans. This finding corresponds with what Echeverria and Zhou observed in [11]. We also extracted user country from the

[3] https://blog.hootsuite.com/twitter-statistics/

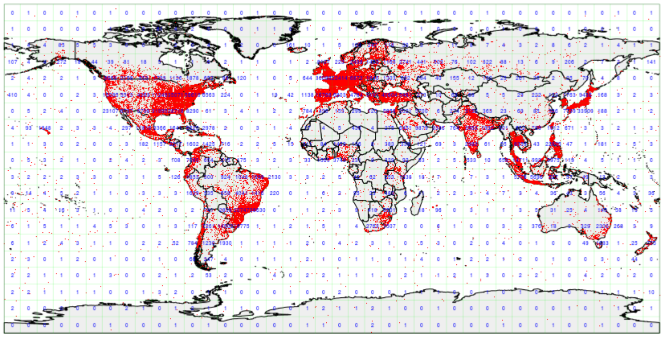

Figure 5: Tweet locations for tweets with coordinates using 40x20 quadrat counting.

user profile information. Out of approximately 9 million users (in our data set) provided location information, only 5.3 million resulted in valid location entries.

D. Botometer Results

Botometer is an online free tool that measure a given Twitter account probability of being a bot[4] [18]. The tool uses machine learning algorithms to classify if an account is a bot or not. Botometer extracts about 1150 features from the user account for classification. Varol et al. showed how these features were selected or calculated [17]. The machine learning framework used in developing this tool is explained in [2] . Yang et al. explained how the detection models were updated and how people are interacting with it [19].

A sample of about 100K of the twitter users we collected was examined with this tool. 16% of the requests returned an error that indicate the user profile has been deleted, suspended, or gone private. This lead us to verifiy the existence of the other user profiles as we will show in the next section.

Figure 6 shows the combined score of the examined users. The highest score is 5 which indicates a bot account where 0 indicates a human account. Around 6% of the examined users have a score of 3.5 or higher. Figure 7 shows the details of the sample accounts. The y-axis represents the number of statuses a user posts, while the circle radius represents the number of followers in logarithmic scale. The users with unidentified scores are drawn in black where other colors indicate the Botometer score. We can see that bots are likely to have different clusters in terms of number of statuses and followers.

E. Deleted or Suspended Profiles

Twitter does not forbid the use of bots; however, they want to prevent the platform from being manipulated[5]. To accomplish that, they improved their spam reporting system to process users reports faster. Also, they employed a spam detection system to detect if an account is participating in platform manipulation activity. If an account is suspected, it will have to go through "anti-spam challenge" before it can be used again. Twitter reported that in 2018 they checked 426 million accounts and 6.7 million are reported to be spam. Hence, we checked the existence of these spamming accounts in our dataset. The analysis show that around 9% of the users are either deleted, suspended, or gone private.

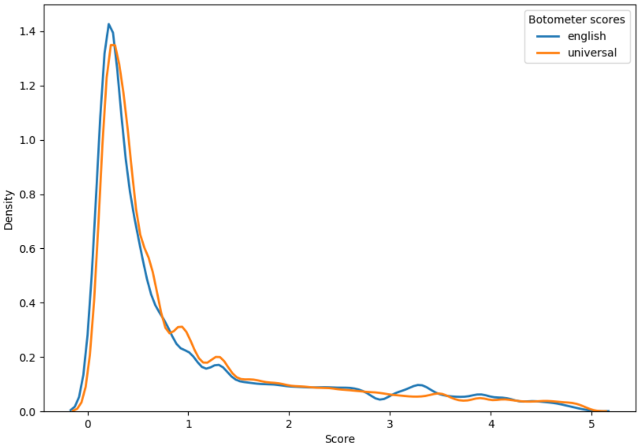

Figure 6: The combined scores of 100K users examined with botometer tool.

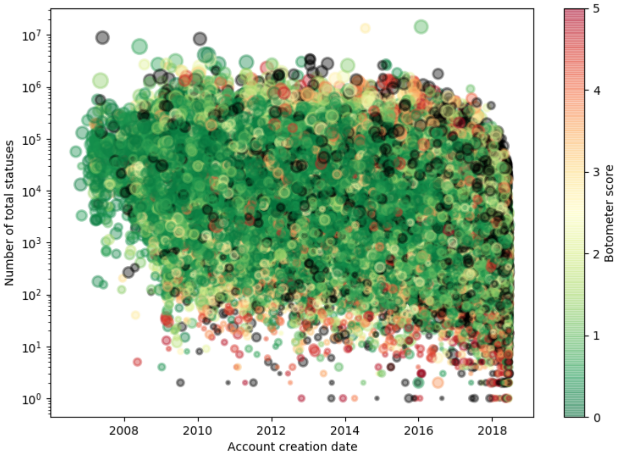

Figure 7: Number of statuses and followers with botometer score and account creation date.

V. CONCLUSIONS

This paper explores and presents some of the initial indicators of social bot behavior during benign events. To this end, we analyzed some of the bot behaviors in Twitter during the 2018 FIFA World Cup. The analysis shows that most of the tweets were posted using handheld devices. It also shows that many tweets were tweeted by using Twitter API. Furthermore, approximately half of the tweets were retweets. We showed that most of the retweets happened within the first day of the original tweet. We analyzed the location coordinates of the tweets and showed the existence of randomly generated coordinates. We confirmed our speculation by testing a sample of our users' dataset

[4] https://botometer.iuni.iu.edu/

[5] https://transparency.twitter.com/en/platform-manipulation.html

against Botometer tool and showed that bots are about 6% of the sample. The analysis indicated that 9% of our users have been deleted, suspended, or gone private which might be a result of Twitter's effort to prevent platform manipulation. Our results show that bots exist even in benign events such as FIFA World Cup Tweets. Their general characteristics seem to follow the attributes found in previous studies. However, we also observe that there seem to be different clusters of bots in our data set. Further research will explore what these different clusters indicate in terms of different behaviours.

Acknowledgement

This research is partially supported by the Natural Science and Engineering Research Council of Canada (NSERC) grant, and is conducted as part of the Dalhousie NIMS Lab at http://projects.cs.dal.ca/projectx/. The first author would like to thank Najran University in Saudi Arabia for his scholarship.

References

[1] T. Inc., "Q1 2019 letter to shareholders," https://investor.twitterinc.com/, 2019, [Online; accessed 1-July-2019].

[2] O. Varol, E. Ferrara, C. A. Davis, F. Menczer, and A. Flammini, "Online human-bot interactions: Detection, estimation, and characterization," in *Eleventh international AAAI conference on web and social media*, 2017. [Online]. Available: https://aaai.org/ocs/index.php/ICWSM/ICWSM17/paper/view/15587/14817

[3] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, "The rise of social bots," *Commun. ACM*, vol. 59, no. 7, pp. 96–104, Jun. 2016. [Online]. Available: http://doi.acm.org/10.1145/2818717

[4] F. Daniel, C. Cappiello, and B. Benatallah, "Bots acting like humans: Understanding and preventing harm," *IEEE Internet Computing*, vol. 23, no. 2, pp. 40–49, March 2019.

[5] C. Shao, G. L. Ciampaglia, O. Varol, K.-C. Yang, A. Flammini, and F. Menczer, "The spread of low-credibility content by social bots," *Nature communications*, vol. 9, no. 1, p. 4787, 2018.

[6] E. Van Der Walt and J. Eloff, "Using machine learning to detect fake identities: Bots vs humans," *IEEE Access*, vol. 6, pp. 6540–6549, 2018.

[7] J. M. Berger and J. Morgan, "The isis twitter census: Defining and describing the population of isis supporters on twitter," *The Brookings Project on US Relations with the Islamic World*, vol. 3, no. 20, pp. 4–1, 2015.

[8] Y. Gorodnichenko, T. Pham, and O. Talavera, ""Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #USElection"," National Bureau of Economic Research, Working Paper 24631, May 2018. [Online]. Available: http://www.nber.org/papers/w24631

[9] C. Castillo, M. Mendoza, and B. Poblete, "Information credibility on twitter," in *Proceedings of the 20th International Conference on World Wide Web*, ser. WWW '11. New York, NY, USA: ACM, 2011, pp. 675–684. [Online]. Available: http://doi.acm.org/10.1145/1963405.1963500

[10] L. Aiello, M. Deplano, R. Schifanella, and G. Ruffo, "People are strange when you're a stranger: Impact and influence of bots on social networks," *ICWSM 2012 - Proceedings of the 6th International AAAI Conference on Weblogs and Social Media*, 07 2014.

[11] J. Echeverría and S. Zhou, "The 'star wars' botnet with> 350k twitter bots," *arXiv preprint arXiv:1701.02405*, 2017.

[12] P. Howard, B. Kollanyi, and S. C. Woolley, "Bots and automation over twitter during the third us presidential debate," 2016.

[13] A. Bessi and E. Ferrara, "Social bots distort the 2016 u.s. presidential election online discussion," *First Monday*, vol. 21, no. 11, 2016. [Online]. Available: https://firstmonday.org/ojs/index.php/fm/article/view/7090

[14] I. Inuwa-Dutse, M. Liptrott, and I. Korkontzelos, "Detection of spam-posting accounts on twitter," *Neurocomputing*, vol. 315, pp. 496–511, 2018.

[15] F. Morstatter, H. Dani, J. Sampson, and H. Liu, "Can one tamper with the sample api?: Toward neutralizing bias from spam and bot content," in *Proceedings of the 25th International Conference Companion on World Wide Web*, ser. WWW '16 Companion. Republic and Canton of Geneva, Switzerland: International World Wide Web Conferences Steering Committee, 2016, pp. 81–82. [Online]. Available: https://doi.org/10.1145/2872518.2889372

[16] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Who is tweeting on twitter: human, bot, or cyborg?" in *Proceedings of the 26th annual computer security applications conference*. ACM, 2010, pp. 21–30.

[17] O. Varol, C. A. Davis, F. Menczer, and A. Flammini, "Feature engineering for social bot detection," *Feature engineering for machine learning and data analytics*, p. 311, 2018.

[18] C. A. Davis, O. Varol, E. Ferrara, A. Flammini, and F. Menczer, "Botornot: A system to evaluate social bots," *CoRR*, vol. abs/1602.00975, 2016. [Online]. Available: http://arxiv.org/abs/1602.00975

[19] K. Yang, O. Varol, C. A. Davis, E. Ferrara, A. Flammini, and F. Menczer, "Arming the public with AI to counter social bots," *CoRR*, vol. abs/1901.00912, 2019. [Online]. Available: http://arxiv.org/abs/1901.00912

[20] S. Wijeratne, A. Sheth, S. Bhatt, L. Balasuriya, H. S. Al-Olimat, M. Gaur, A. H. Yazdavar, and K. Thirunarayan, *Feature Engineering for Twitter-based Applications*. New York: Chapman and Hall. Data Mining and Knowledge Discovery Series, 2018 2018, ch. 14, pp. 359–393.

[21] D. de Leng, M. Tiger, M. Almquist, V. Almquist, and N. Carlsson, "A second screen journey to the cup: Twitter dynamics during the stanley cup playoffs," in *2018 Network Traffic Measurement and Analysis Conference (TMA)*. IEEE, 2018, pp. 1–8.

[22] C. Shao, G. L. Ciampaglia, O. Varol, K.-C. Yang, A. Flammini, and F. Menczer, "The spread of low-credibility content by social bots," *Nature communications*, vol. 9, no. 1, p. 4787, 2018.

[23] A. Baddeley *et al.*, "Analysing spatial point patterns in r." Citeseer, 2008.