Projet de Fin d'Études
2014 – 2015 | [R|E]

D1.1 – Final Report

Analyzing Twitter: Whom can we trust?

Participant:
Mourjo Sen
Email: sen.mourjo@etu.unice.fr

Supervisors:
Arnaud Legout
Maksym Gabielkov
Email: { **arnaud.legout**, maksym.gabielkov } @inria.fr

Université Nice Sophia Antipolis

POLYTECH NICE-SOPHIA

Abstract

Twitter is a popular microblogging service that enables users to send short messages ("tweets"), most of which are public. Users can follow each other to receive these tweets, which creates a directed graph of information flow. Much like any other information source, the question of how trusted some information source is (users, in this case) is of primal importance. In this project, we study the Twitter social graph to look for ways to identify users who can be "trusted", that is, users who are who they say they are and whose posts can be considered genuine. The goal of the project is to find a reasonably sized and justified set of trusted users on Twitter, apart from the users already verified by Twitter itself. We do this by analysing characteristics of the users and their position on the social graph. The set of users, who have been verified to be genuine by Twitter, typically consists of celebrities and notable businesses. We use a metric to serve as proxy for the subjective notion of trust, called the ***trust score****. This metric was developed in the PFE of Master 1. We categorized unverified users as trusted or not based on their trust scores assuming that verified users can be trusted. In this project, we collect more data from Twitter in 2014 to analyse the trust score mechanism and show that it is indeed a valid metric of trust and that it can change with the changing parameters of the social network of Twitter.*

Contents

1 Introduction

Twitter is a very popular online social networking and microblogging service that enables users to send and read short 140-character text messages, called “tweets” [1]. Most of these messages are public and can be viewed without even creating a Twitter account. Twitter has more than 537 million users and about 255 million monthly active users [2].

On Twitter, users can follow one another to automatically receive any tweets posted by the user being followed. The follow relationship is not symmetric and therefore a person following another person does not mean that the converse is true. In other words, the links on the Twitter social graph are directed. So, Twitter is also considered as a news medium along with a social networking medium [3]. This makes Twitter different from other social networking sites like Facebook, which primarily uses undirected links between users resulting in the symmetric relationship of “friendship”. Of course, symmetric relationship can be achieved on Twitter when two users follow each other. Therefore, Twitter is more general and is closer to how information propagates in real life [4]. But it has been found by H. Kwak et al. that following is mostly not reciprocated [3]. Rather, there are a few users who have many followers and can therefore directly reach a large audience. This aspect can be thought of as the “fan relationship” in real world. That is, celebrities have a lot of fan following, but ordinary people have few. The asymmetric relationship found in Twitter models this asymmetric relationship, as well as the symmetric friendship relationship. It is because of the presence of these two types of general relationships in Twitter that we believe that it can be a good model of social networking in general and hence we want to study the aspect of trust in Twitter in this project.

2 Motivation

There are about 500 million tweets published every day [2]. It is easily possible for someone to pretend to be someone else (impersonation) on the internet and/or publish fraudulent information with malicious intent or for unethical professional gain, or simply to create rumours [5]. Therefore, it is very important for any information source (here users publishing tweets) to be proved authentic and trustworthy. There have been incidences of social media hoaxes that have had serious sociological connotations in recent years. From creating rumours of actor Morgan Freeman's death [22] to a teenage girl's kidnapping hoax [23] – all have been fuelled by the quick, unchecked and effortless diffusion of information in social networks in the wild. In fact, Twitter has been used for illegal financial activities like stock market fraud as well [25]. With more than five hundred million users on Twitter, it is almost impossible to manually verify the identity of every user who signs up on Twitter and it is even more difficult to keep track of users who tend to spread information of questionable authenticity, unknowingly or deliberately. Therefore we need to identify trustworthy users on social networks like Twitter. This is the principal motivation behind this project.

The ultimate goal of this work, which will be addressed during the internship, is to classify tweets as trusted or not. Being an information broadcasting mechanism, information on Twitter can quickly become viral. This has been manipulated in the past for personal and professional gains. The strong incentive to manipulate perception of public opinion lies in the fact that Twitter has an increasing impact on society.

3 Goal of the Project

Some users on Twitter have been manually verified by Twitter following administrative processes of cross-checking their profile with their identity. Mostly verification is done for public personalities and celebrities who are famous. According to Twitter, "Verification is currently used to establish authenticity of identities of key individuals and brands on Twitter" [6]. Twitter certifies that these verified users are trustworthy. But only a very small fraction (0.01%) of users is verified by Twitter, and it leaves the remaining 99.99 % of users, whose authenticity and legitimacy cannot be guaranteed by the lay man. 99.99 % of Twitter cannot be untrusted. We have already done a part of the work in last year's PFE for Master 1, in which we found a trust metric to measure how trusted a user is. For this project, our goal is to analyse the trust metric and validate our method by showing that it indeed upholds characteristics of being trusted and can identify users who are authentic.

We also want to show that our method can incorporate the changing dynamics of Twitter over time.

4 Paper Organisation

This report is divided into four major sections – first we talk about the current state of the art. Then we describe the workflow of the project and the timeline, following which we talk about our trust score, and how it is calculated. Lastly we describe how we justify and validate our method of finding trusted users on Twitter and the challenges faced in doing so.

5 State of the Art

A significant amount of work has been done on how to find trusted users in a network and ensure network security. We focus on finding trusted users on social networks like Twitter. Techniques such as chi-square distributions [19], SVM-based methods [13, 14] and machine learning techniques have been used to estimate trust [15]. TwitterRank [16] is another approach which is based on the PageRank algorithm to find influence of users on certain topics. Pal et al. [20] have used features of the Twitter graph and analysis of tweets to deduce if a user has significant contribution to a topic, which gives them a level of trust towards that user in that field.

Twitter has its own "who-to-follow" service which uses information from a user's profile to find popular users with the same field of interest. According to Twitter, these suggestions are based information like email and/or phone contacts, contacts of contacts and patterns detected from history of behaviour on Twitter [18]. Of course, the users suggested by Twitter have either personal relation (like phone contacts) with the user or have had a significant impact on Twitter social network and can thus be assumed to have a trusted status.

Naveen Sharma et al. [9] have created a "who-is-who" inference service (deployed on the Web at http://twitter-app.mpi-sws.org/who-is-who/) using Twitter data to deduce particular attributes about users. The information deduced from Twitter by the "who-is-who" service not only uses information in users' Twitter profiles but also their areas of interest and expertise. Moreover, it computes popular view about users on Twitter.

Most approaches before Naveen Sharma's work concentrated on information about users from content that is produced by the user themselves, like profile information, biography, and tweets [17]. But such information may not be accurate in describing whether a user can be trusted or not because such content can easily be manipulated by users with malicious intent. Naveen Sharma et al. therefore used a different approach to analyse the online personalities of users on Twitter. They used Twitter lists, which are groups of Twitter users created by a particular user to manage tweets related to similar topics. According to Twitter, one can create one's own lists or subscribe to lists created by others. A list timeline shows a stream of tweets only from the users on that list [11]. Many users use lists to categorize the people who they want to follow. Thus, if a user appears on many lists, it would suggest that the user is popular.

The work of Naveen Sharma et al. was to examine the meta-data of Twitter lists in which a user appears. That is, to study how popular a user is, and more importantly to study in what field a user is popular in, Naveen Sharma et al. used the information about the lists themselves to gather a user's field of popularity, and not just popularity as a whole. This gives more insight because social networks are highly clustered and people are often only popular among people having similar interests. Attributes of users found using this method include their field of popularity or expertise, interests, professional details, "known for" attributes. For example, Lance Armstrong may state in his profile that he is a noteworthy sportsperson but details about events like his participation in Tour de France and association with cancer can be deduced by studying the lists he appears in. But whether this correlates to the issue of trust has not been studied.

In their study, Naveen Sharma et al. divided popular users, found using their technique, into three classes based on the information gathered using their technique: well-known users, news and media users and US senators. They found a set of users whom we call experts, who have a high influence on Twitter because they are related to a certain domain where they are popular. Amongst these users, there are users who are experts on very niche topics, such as robotic space exploration, and stem cells. They have had a considerable impact on the Twitter social graph. We will use the set of experts in assessing our trust metrics. Analysis of the results of this study showed that very popular users, i.e. users with a high number of followers, are mentioned in lists quite frequently. The number of mentions in lists falls quickly as the number of followers decreases.

There are users in Twitter who have been verified by Twitter and constitute a small fraction of the total population of users in Twitter. Verification is only initiated by Twitter and it cannot be requested by a user. It is typically performed for celebrities and public figures, including notable businesses. We consider a verified user to be trusted (relative to an unverified one), since to earn verified status, they must use their real-life identity and be sufficiently well-known by the general public for Twitter to consider that there is a risk of someone impersonating them. As stated by Forbes.com, several businesses have been impersonated, with imposters posting tweets that threaten to malign their business's reputation [1]. The verified status is thus a mechanism to uphold the integrity of the user's identity. Therefore we consider a verified user to be trusted.

After the work done by Naveen Sharma et al., the structure of Twitter has gone through a few changes. Naveen Sharma's work was based on Twitter data from 2009, collected by Kwak et al. [3]. As studied by Maksym Gabielkov et al. [4], Twitter has changed since then.

- The 2009 dataset (along with other previous data sets) was not exhaustive/complete and there were subtle properties that were not visible in the 2009 dataset [4].
- There was a major change in the Twitter graph in 2009-2010, when a large number of celebrities joined Twitter and its popularity started increasing manifold. Celebrities are not interested in following too many people, but they have a high number of followers. This changed the properties of the Twitter graph in 2009-2010. These changes were not reflected in the 2009 dataset [3] used by Naveen Sharma et al.
- There has been a tenfold increase in the size of Twitter since 2009. Twitter today is one of the most popular social networking sites on the internet [7].

Thus, for the project we have to use more recent datasets. The dataset collected by Maksym Gabielkov et al. [8] represents Twitter of 2012. They used distributed crawling with 550 PlanetLab nodes to collect the dataset. This dataset contains the entire Twitter graph of 2012, i.e., every user on Twitter and their connections. This dataset is significantly more comprehensive, exhaustive and more representative than the 2009 dataset. We used this dataset in the project.

6 Timeline of the Project

This project is divided into three stages. In the first stage, we define a metric of trust, in the second stage, we analyse the metric and show that it is a good way to measure trust, and in the third stage, we apply it to classify tweets as trusted or not. I have worked on this project for the PFE of Master 1, last year, and finished the first stage. This PFE is a continuation of the work that was done last year. The internship on the same project is planned for the last stage.

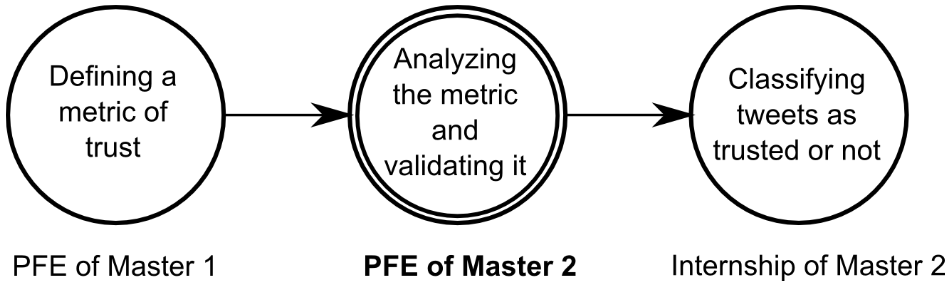

Figure 1: Stages in the development of the project. We completed the second stage in the Master 2 PFE.

6.1 PFE of Master 1

Last year, we explored a set of metrics which we believed would be a measure of trust in social networks. After closely investigating each of the explored metrics, we found that the metric we call "trust score" is the best metric to quantitatively summarize the subjective notion of trust. We will use this trust score metric in this project as well, and show that the metric is indeed indicative of trust. Using the trust score metric once can measure how trusted a person is, and it can enable consumers to decide who to listen to (follow) and who to avoid. We explain the details of the trust score later in this report.

6.2 Timeline of this Project

The time available for this PFE was four fulltime weeks, and some extra time between courses. We recorded the progress of the project in the number of weeks. There were specific tasks completed each week and logged. The following table shows a summary of the accomplished tasks by week. Each task is explained in detail later in the report. This table is just to show the timeline.

Week	Tasks performed
Week 1	• Review of the state of the art, selected papers, reading existing methods, reading the Twitter REST API documentation • Collection of all verified users in 2014
Week 2	• Comparison of verified users of 2014 to the verified users of 2012 • Investigating the overlap of trusted users of 2012 and the verified users of 2014
Week 3	• Estimation of the size of Twitter today • Comparison of method of estimation to the full 2012 dataset
Week 4	• Collection of trusted users by our method in Twitter today • Analysis of these users compared to others
Week 5	• Investigation of exceptions in the trusted set • Final recalculation and verification of computations

7 The Trust Score

Though "trust" is a subjective topic and is open to interpretation, for this project, we define being trusted as the likelihood of being who one claims to be, that is judging by a person's position on the Twitter graph, how probable it is that he/she is who he/she claims to be. By using this notion of trust we hope to identify legitimate users on Twitter, who create trustworthy tweets. To quantitatively estimate the inherently subjective notion of trust, we use a metric called the "trust score", which is based on the number of verified followers a user has. More number of verified followers means more trusted the user is. For this project, any user with more than one verified follower is included in the "trusted set" of users. We would like to make a clarification here that the set of verified users does not overlap the set of trusted users. Even if a verified user has a verified follower, because he is already verified, he is not included in the trusted set. Therefore, these two sets are distinct and disjoint. The set of verified users are found by Twitter by a manual administrative process whereas the trusted set is found by us in an automated process. The trusted set is much more inclusive than the verified set, which only contains 0.01% of all users on Twitter.

Since verified users have been certified by Twitter to be trusted and legitimate, we assume that a verified user will not follow someone who is known to be a fraud or an impersonator. Trust is imparted to a unknown user X by a verified user when the verified user decides to follow the user X. Imparting of trust is seen in other fields as well – consumers are more likely to believe what someone they trust says about a product rather than a marketing promotion of the same product. The notion of trust score is an extension of this – we know the verified users to be trusted, and when they follow someone, it imparts a value of trust onto the followed user. In the following sections we will show that the trust score, albeit a simple one, is a good metric to measure trust.

The main objective of the project is to show that using the trust score to identify trusted users is reliable, and to validate it by showing that it can identify characteristics that are expected to be found in trusted users.

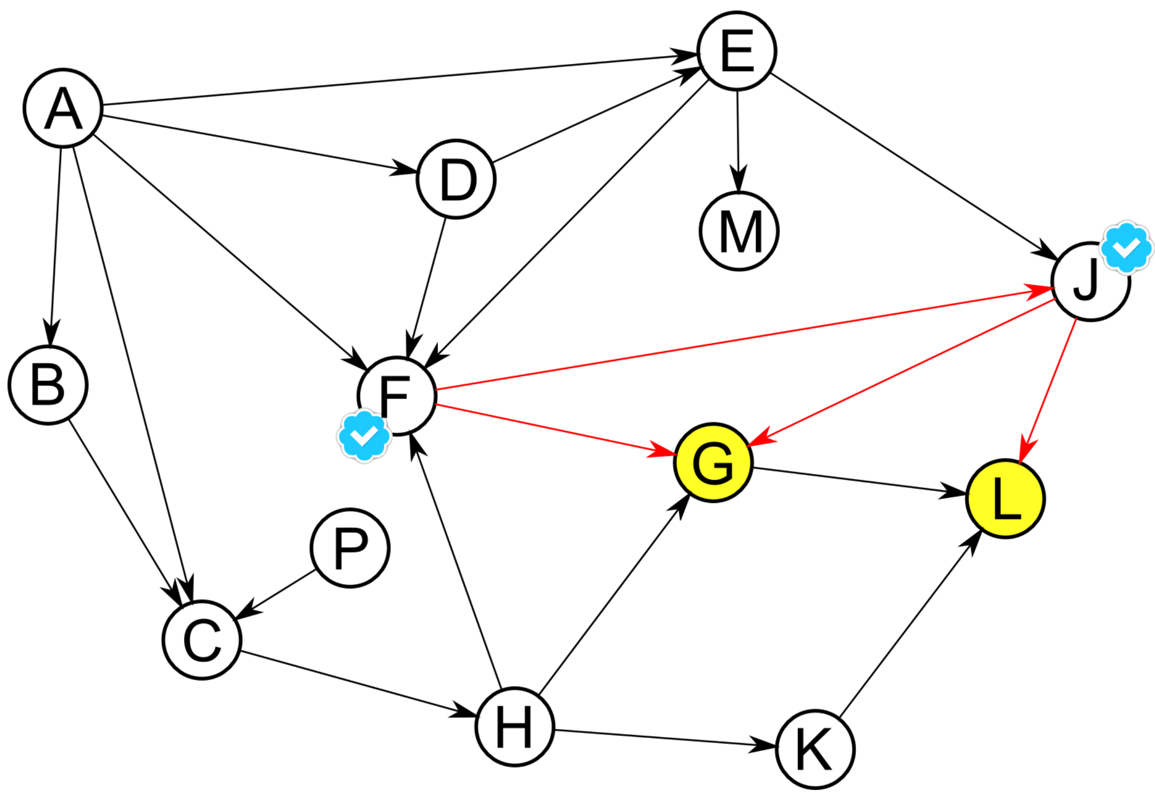

Figure 2: A graph similar to the Twitter graph, with two verified users F and J. A link in this graph from X to Y means that X follows Y. The outgoing links (in red) from the verified users are used to find the trusted users. G and L are the trusted users with a trust score of 2 and 1 respectively. So G is more trusted than L. Verified users are not included in the trusted set.

8 Tools and Datasets Used

We used two datasets primarily in this project. We used the complete Twitter dataset of 2012 collected by Maksym Gabielkov et al. [8]. This was used mostly to find trusted users in Twitter in 2012. We then partially collected the Twitter dataset in 2014 to see how the trusted set evolved over time from 2012 to 2014. We used the 2014 dataset to show that our method can adapt to changing dynamics of the Twitter social network over time. We collected the verified users of 2014 and the trusted users of 2014. To collect data from Twitter, we used Twitter's REST API [24]. There are many calls that the API provides for different types of data, which we used for collecting the data. We used a random sampling technique to collect some portions of the graph in 2014, as we will explain in the following sections. The reason we could not collect the full dataset of Twitter in 2014 is because of the huge size of Twitter, and the rate limitations imposed by Twitter's REST API which made it practically impossible to crawl the entire Twitter graph without using any specialized infrastructure like NEPI [21].

9 Analysis and Results

In this section we describe in detail the tasks that were performed during the course of the project to show that the trust score method is a valid method of measuring trust in Twitter. While doing the project we asked ourselves three fundamental questions, answers to which were the work of the project, to validate the trust score method:

Is a trusted user more likely to be verified than other users? The answer to this question would validate our method, because that will correlate Twitter's manual verification process to our automated process. To find the answer to this question, we collected the set of verified users of 2014, and compared it to the trusted set that we had found on the 2012 dataset for any overlap. This is described in section 9.1.

Can the set of trusted users stand the test of time? To answer this question, we had to find the size of Twitter to be able to compare if the trusted user set remains static or changes as Twitter itself changes over time. We explain this in section 9.2. Then we compared the change in the size of Twitter and the trusted set from 2012 to 2014. This is explained in section 9.3.4. We then compared the trusted sets of 2012 and 2014 to see how much has changed and the effect of time and the dynamics of the trusted set, as explained in section 9.3.5.

Are the trusted users more popular than other users? The reason we wanted to answer this question is because if the trusted users are not followed by other users, it means that the trusted users have no impact on Twitter, and therefore if they are genuine or not does not really matter. We answer this question in section 9.3.3.

9.1 Verified Users of 2014

Twitter has an account with the screen name @verified (https://twitter.com/verified). This account, while itself being verified, follows all other verified accounts on Twitter. As the description says on the @verifed account, the @verified account follows "accounts verified by Twitter". We used the Twitter REST API to get all the users followed by this account to collect the verified user set. At the time when we did it (Nov 2014), there were 113,654 verified users in Twitter. We found that the *percentage* of verified users in 2014 has increased from 2012 by 1.6 times, and this suggests that Twitter is actively verifying users to increase the proportion of authentic users in Twitter.

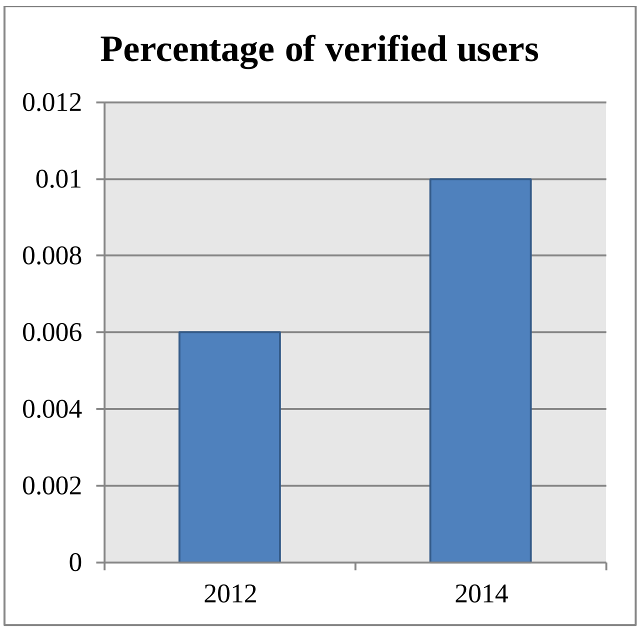

Figure 3: Increase in the percentage of verified users from 2012 to 2014 indicates that Twitter is actively verifying users to have higher proportion of certified authentic users

We then compared the verified set of 2014 to the trusted set of 2012. We found that 60 %[1] of the new verified users of 2014 are from our trusted set of 2012 that we calculated. That is, using our method, we could anticipate in advance which users are likely to be verified manually by Twitter. The trusted set of 2012 was just 4.6 % of the entire Twitter graph, and to find **60 % of the new verified users from 4.6 % of Twitter that we indicated as trusted**, shows that our method is quite efficient in finding authentic users and Twitter's manual verification process agrees with it. Twitter has dedicated teams to manually verify users, whereas our method was automated, and involved no manual checking of users for being included in the trusted set. **Thus, our method not only strongly correlates to Twitter's verification process, but also does it automatically.**

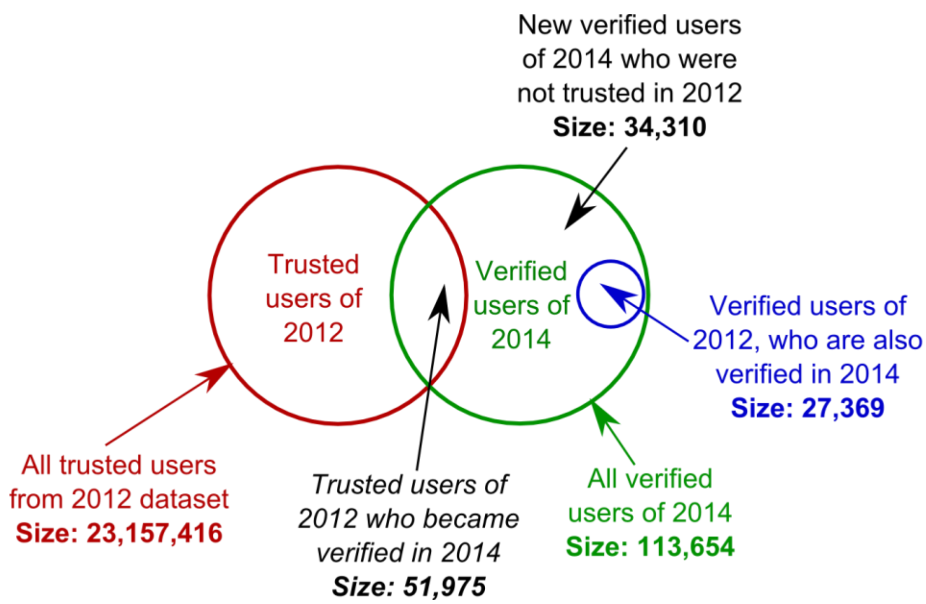

Figure 4: Venn diagram to show that 60 % of the new verified users of 2014 were from the trusted set of 2012

9.2 Size of Twitter in 2014

We estimated the size of Twitter in 2014 in order to be able to compare how the size of the trusted set of users in 2014 as a percentage to what it was in 2012, and also to be able to confirm that the trusted set is of a reasonable size, and that it is not as restricted as the verified set found by Twitter. We used a random sampling method to estimate the size of

[1] There are some verified users of 2014 who did not exist in 2012, and the 60% does not take that into account.

Twitter, because it was not possible to collect all users because the Twitter REST API has a very restrictive rate limit 12 requests per minute.

We divided the ID space into two sections, for two types of sampling:

1. **Users from 2012 dataset:** We had the full dataset of 2012, so we only had to find the users who deleted their account on Twitter. We queried the API with the IDs of the 2012 users we had, to check if they still exited in 2014. We selected 507,780 IDs from the 2012 dataset at random and found that 94 % of them existed in 2014. Then, since we had the total number of users in 2012, we applied this probability of existence (94 %) and estimated the number of users from 2012 who existed in 2014 to be 474,886,862.
2. **New users of 2014:** We had no data for the users of 2014 who did not exist in 2012. Therefore we had to use a random sampling of higher rate to estimate the number of new users in 2014, who did not exist in 2012. First we noted the maximum ID of the 2012 dataset – this was used as the lower-bound of the ID space of the new users of 2014. For calculating the upper-bound of the ID space of the new users of 2014, we created a new user on Twitter and used this user's ID as an approximate upper bound, as IDs in Twitter always increase. Once we had the upper and lower bounds of the ID space, we generated 2,166,116 random numbers in this range and checked if these numbers corresponded to an existing user in Twitter. We found that around 30 % of these numbers corresponded to existing users. The size of the new user set in 2014 was estimated by applying the probability of existence (30 %) on the whole ID space (i.e., upper bound - lower bound), and it was found to be 649,315,258. The ID space from this sampling is shown in Figure 5. In the X-axis, we have the IDs sampled, and in the Y-axis we have the percentage of IDs corresponding to an existing user.

So in total, the estimated size of Twitter in 2014 was calculated by adding the estimated size of the two ID spaces, and was calculated to be **1,124,202,120.**

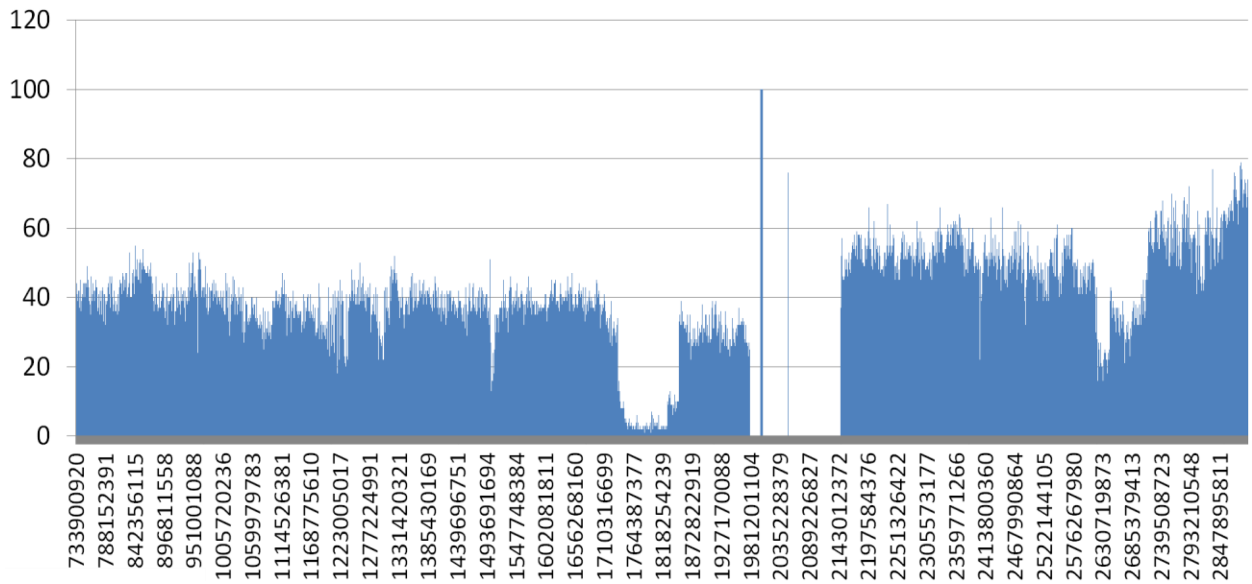

Figure 5: The distribution of the ID space of Twitter users in 2014. In the X-axis, we have the IDs sampled, and in Y-axis we have the percentage of IDs corresponding to existing users in Twitter in the range (all ticks are not shown in the X-axis).

9.2.1 Evaluation of the Sampling Technique for Users of 2014

To validate the method of random sampling of user IDs for estimating the number of new users in 2014, we applied the same technique to find the number of users in the 2012 dataset. That is, we generated random numbers between the highest and lowest IDs in the 2012 dataset, and since we had the full dataset, we checked how many random numbers correspond to an existing user. We found that the result of the sampling technique was 94 % of the total number of users in the 2012 dataset, thus validating our sampling technique, as 94 % is fairly accurate for our purposes.

9.3 Trusted Set of 2014

As we explained before, the trusted set of users are those users who have at least one verified follower. The trust score for a user is the number of verified follower that a user has – higher the trust score more trusted the user is. In this section we talk about the trusted set of users in 2014 and their properties.

9.3.1 Collection of Trusted Users of 2014

The trusted users were collected by following the outgoing links from the 113,654 verified users in the Twitter graph. This was particularly difficult to achieve since we had to find all users who were followed by each of these 113,654 verified users and it often required more than one request for a verified user, because the API returns followed user IDs in groups of

5000 IDs. On top of that, the API had a rate limit of only one request per minute. So even if we assume that only one request would be required per verified user to collect all the trusted users of 2014, it would still take 79 days to finish. We therefore devised a parallel crawler, which had 31 threads, each collecting only a part of the trusted set. Using this, it was possible to find the entire trusted set of 2014 in three days. The trusted set of 2014 contains **71,701,828** users, which is 6.38 % of the 1.1 billion estimated users in Twitter in 2014.

9.3.2 Trusted Users by Trust Score

We investigated how many trusted user had a given trust score (number of verified follower). As shown in the figure below, the number of trusted users decreases exponentially as the trust score increases.

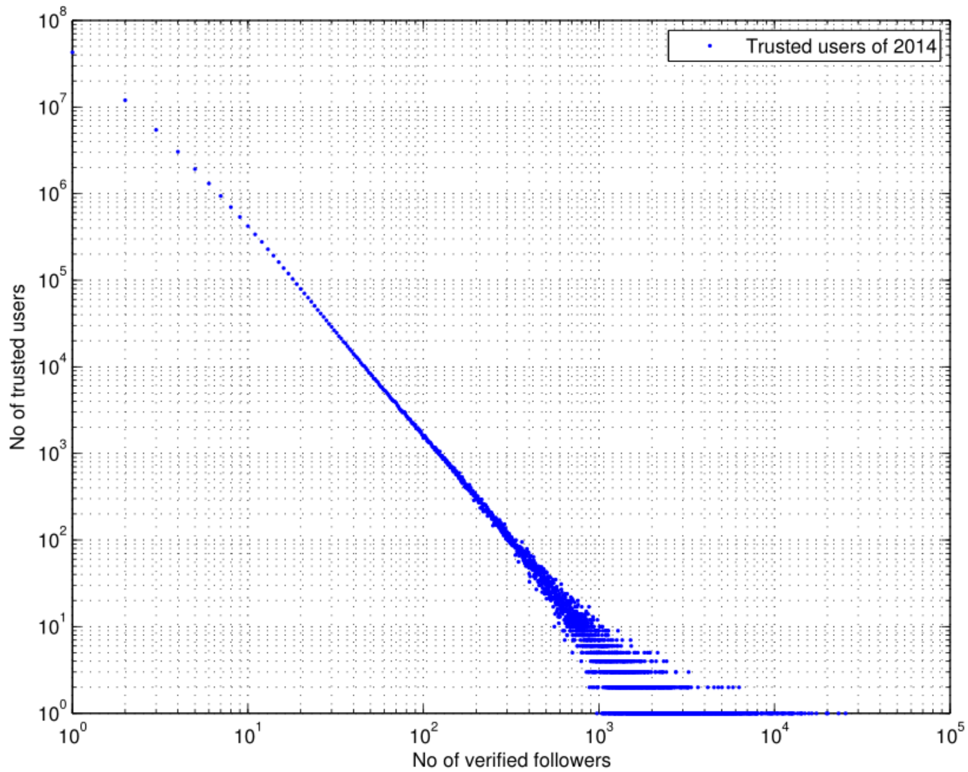

Figure 6: Trusted users of 2014 according to number of verified followers (log-log scale)

9.3.3 Popularity of Trusted Users of 2014

Another question we wanted to answer about the trusted users is if they are popular on Twitter. If trusted users are not popular, and no one follows them, then whether they are trusted or not is an irrelevant question, because no one on Twitter would be impacted by it. Thus by being popular, we consider the number of followers a user has. To answer this question, we plotted a CDF of the number of followers for verified users, trusted users and other users, as shown in the figure below. It can be observed that the trusted users have a fairly high number of followers. The verified users have the highest number of followers and that is not surprising because they are mostly celebrities and famous personalities, and inherently have a fan following. The trusted set, interestingly, has much more followers than other users.

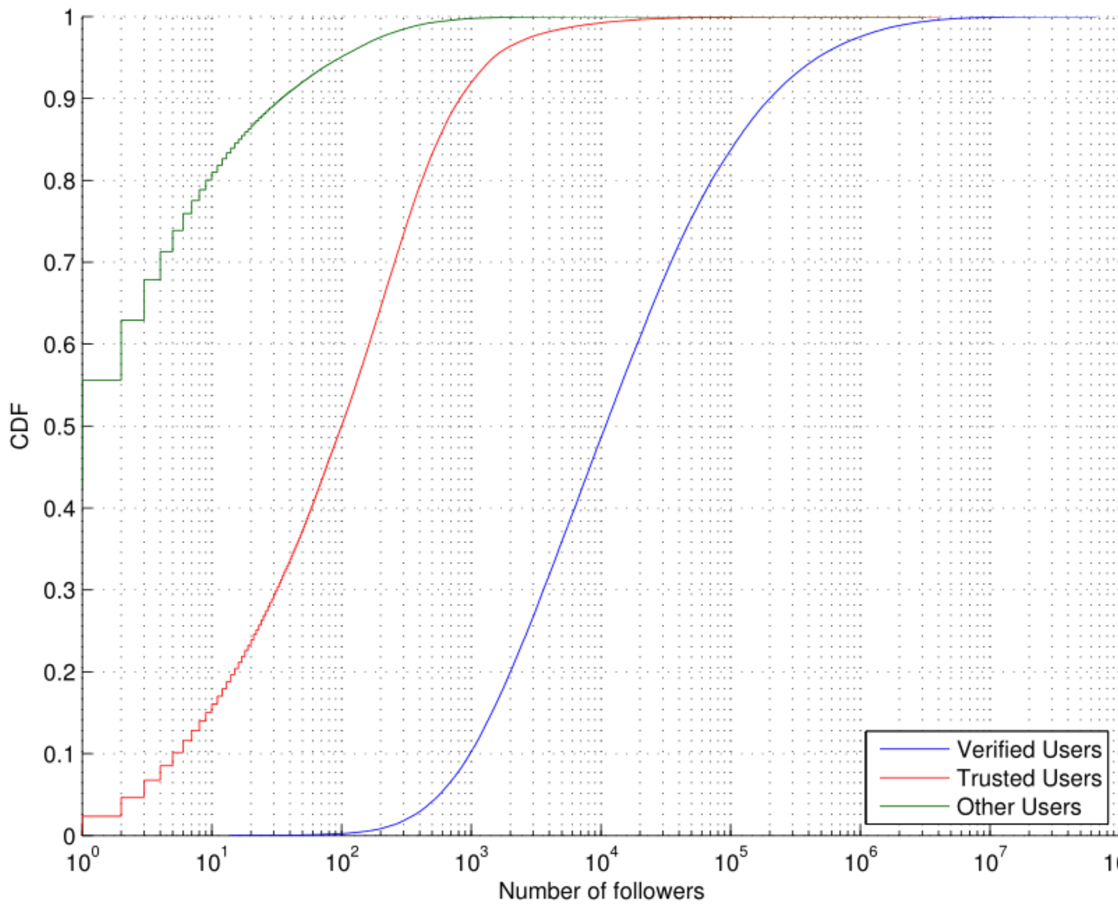

Figure 7: CDF of the number of followers for three categories of users - verified, trusted and other users. This shows that the trusted users are more popular than other users.

To further the claim that trusted users are active, we then plotted the reciprocation behavior of trusted users compared to verified and other users. By reciprocation we mean the ratio of the number of users followed by a user to the number of users following that user. That is, the ratio of the number of outgoing links to the number of incoming links per user. And as the figure below depicts, we see that the trusted users reciprocate more than verified users, who because of the virtue of being famous, are followed by more users than they themselves follow. Thus, the trusted set is both popular and active on Twitter.

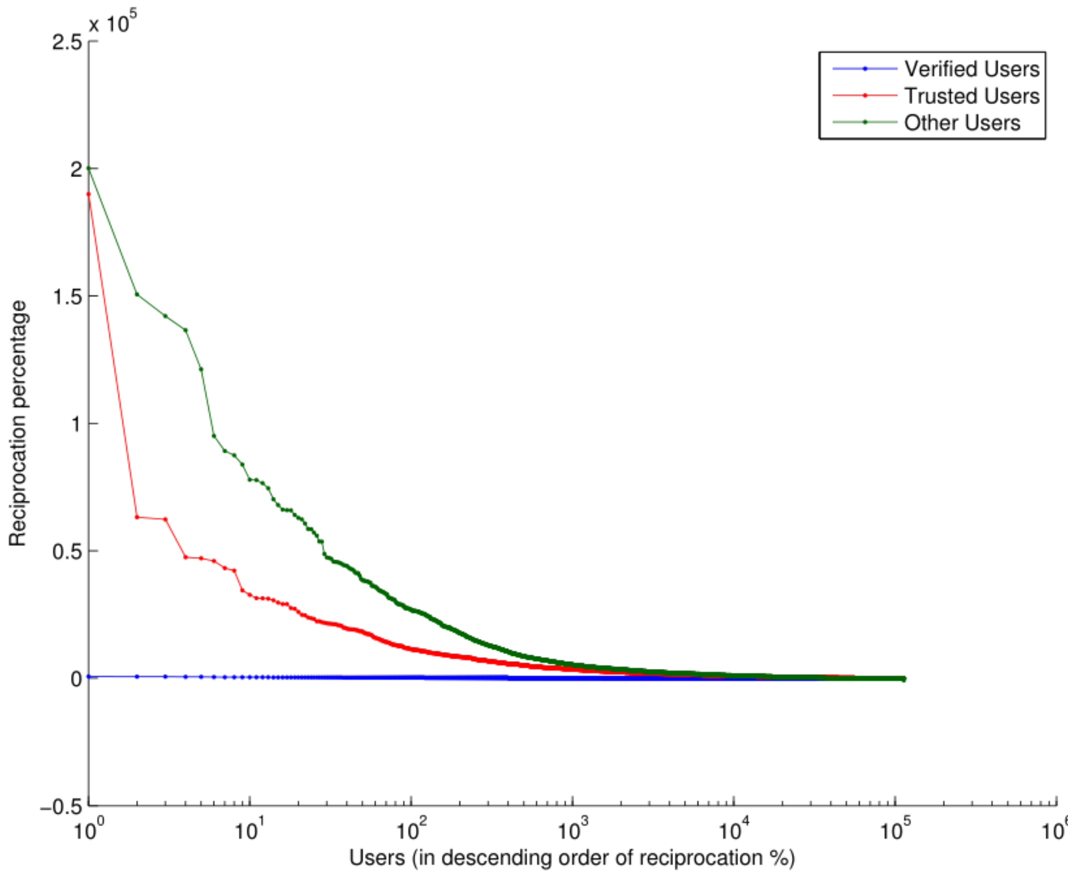

Figure 8: This figure shows that verified users reciprocate the least, and trusted users reciprocate less than other users

9.3.4 Changes in the Trusted Set over Time of 2014

To determine if the trusted user set is a static set or not, we compared the change in the size of the trusted set from 2012 to 2014. We found, as shown in the following figure, that as the size of Twitter increased from 2012 to 2014, so did the size of the trusted set of users. Thus the trusted set is not a static set, and it evolves with time.

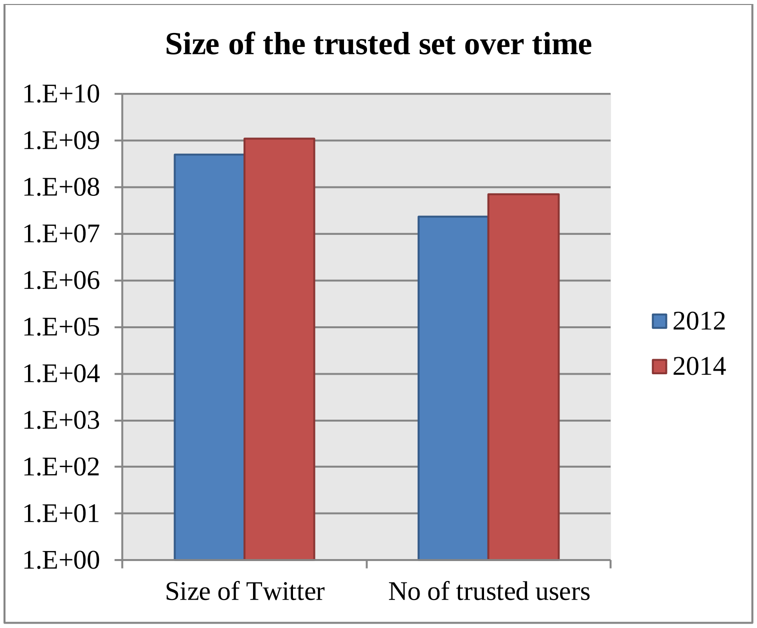

Figure 9: The size of the trusted user set increased with the increase in the size of Twitter

We also investigated if a higher proportion of trusted users in Twitter in 2014 compared to 2012. We found that the percentage of trusted users has increased from 2012 to 2014, and this is most probably owing to the increase in the percentage of verified users from 2012 to 2014.

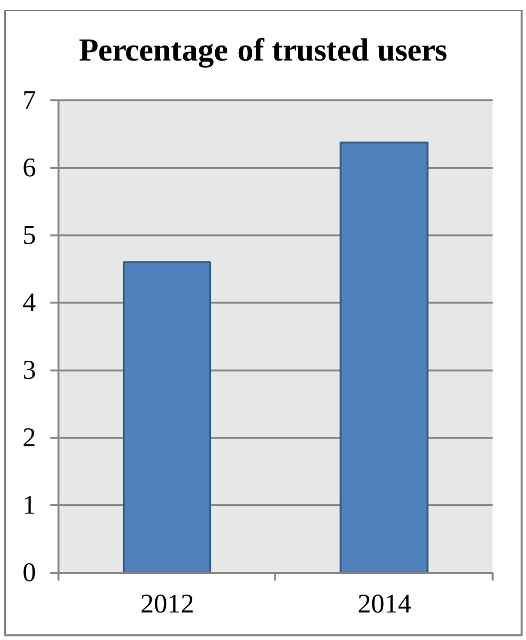

Figure 10: A higher proportion of users were found to be trusted in 2014 than 2012, showing that Twitter is actively trying to verify users to increase the amount of trust in their social network

9.3.5 Missing Trusted Users: Dynamics of the Trusted Set

We found that some trusted users of 2012 were not included in the trusted set of 2014, although they exist in 2014. This comprised 8.3 % of trusted users of 2012 and we called them the missing trusted users. This is not an anomaly – instead, this is proof that the trusted set of users is a dynamic, evolving set. These missing users may have lost their trust certification because of two probable reasons:

1. The verified status of the users who followed the missing user in 2012 were revoked the verified status by Twitter. This may be because these verified users were no longer authentic and genuine as Twitter initially thought. And because of that, the missing user also lost its trust, because trust is seen as a transitive relationship in this project – the verified user trust imparts trust onto the users who he/she follows. When this verified user loses his credibility of verification, the users followed by him, by the transitive relation, also lose credibility.
2. The verified users who followed the missing user stopped following him/her. This maybe because the verified users realised that this missing user is in fact an imposter/fraud, and were thus they were not interested in them anymore. This is a strong validation of the dynamic nature of the trusted set.

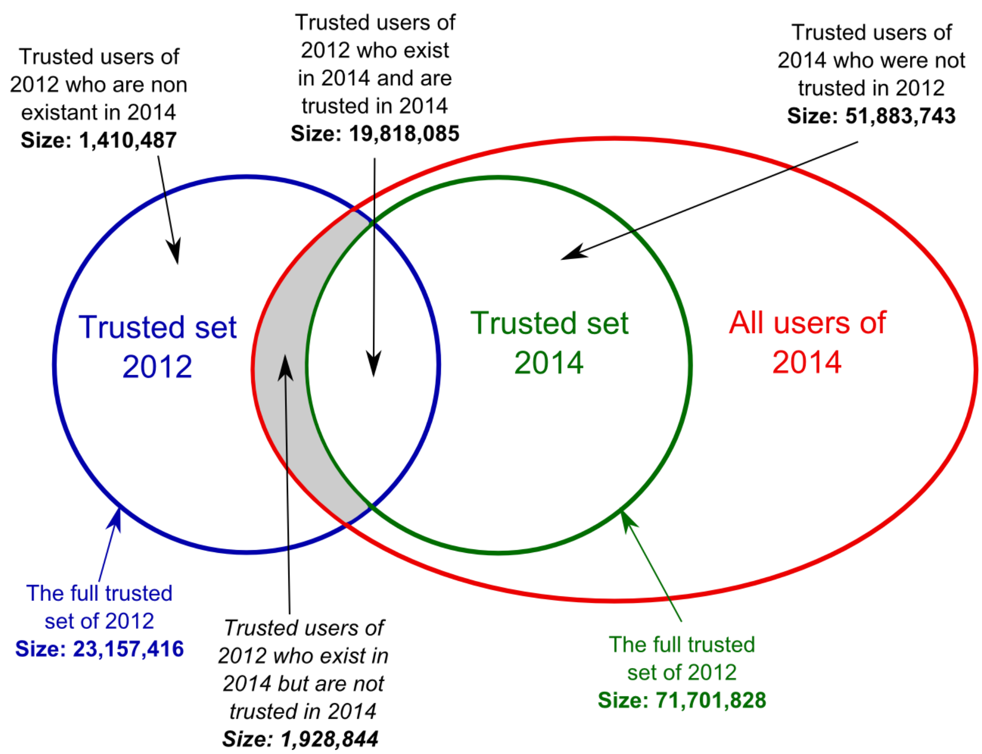

Figure 11: A Venn diagram to show that some users who were trusted in 2012 are not trusted in 2014 although they exist in 2014

We found that in 2012, the missing trusted users had a lower trust score than the non-missing trusted users, as shown in the figure below. The figure is a CDF plot of the 2012 trust score of the missing users and the non-missing users. It shows that the users who are missing from the trusted set of 2014 had a lower trust score in 2012. Thus, trusted users having lower trust scores can become untrusted over time more easily than trusted users having higher trust score, and this is exactly the semantics behind the trust score – higher the trust score, more trusted the user is, and thus less likely to become untrusted over time.

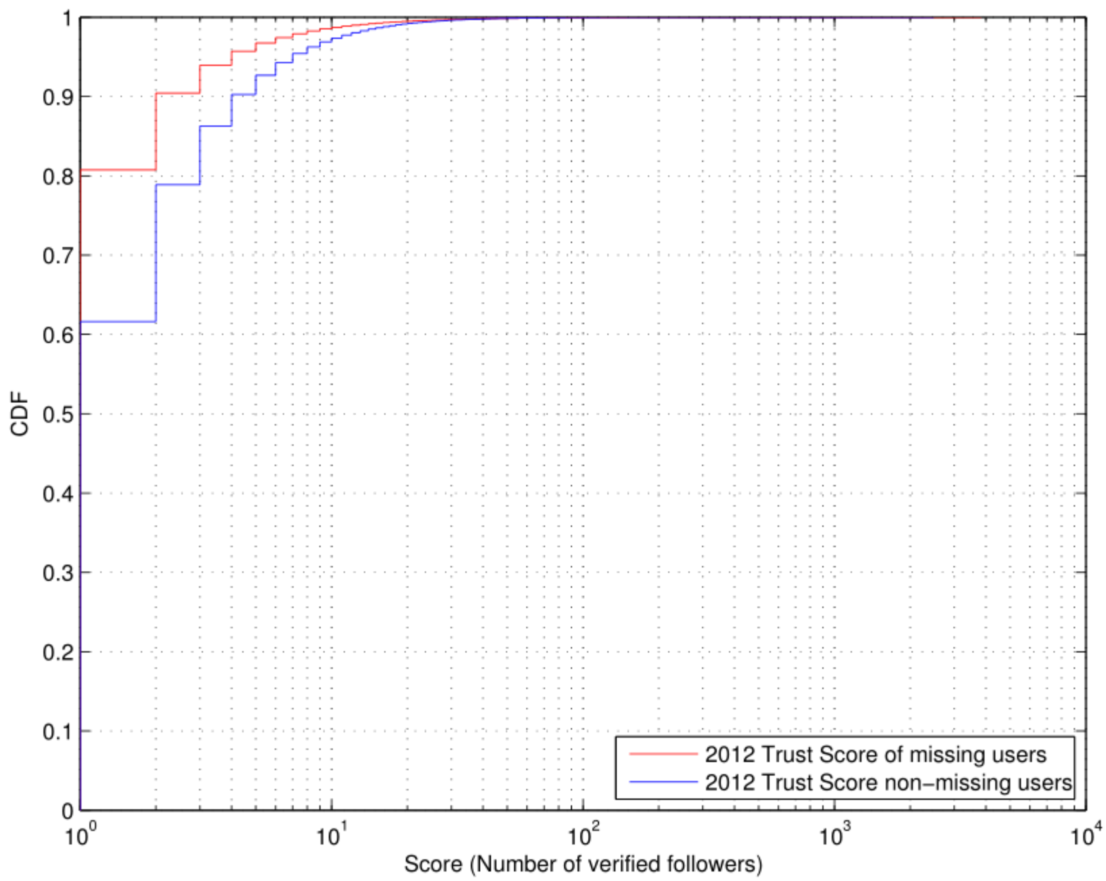

Figure 12: 2012's trust score of missing users and non-missing users. This figure shows that the users who are missing from the trusted set of 2014 had a lower trust score in 2012.

10 Challenges Faced

The first problem that was faced is the rate limitation of the API provided by Twitter. We had to devise workarounds to solve this problem. As we mentioned before, collection of the trusted users was particularly difficult in this regard, as the size of the trusted set is huge and the API provides only a rate of one request per minute. Apart from the rate limitation, there was also the problem of constant collection. Since the collection of the trusted users lasted almost three days, there was a need to have a persistent connection with the API for three days, which was not a trivial problem because we had to use the internet connection provided at my student residence, which reset every 6 hours, and required authentication. We had to write a script to work around that as well. The second problem we faced was that there was no way to load all the trusted users' data into memory, because of its huge size. So for most tasks, we had to devise algorithms that could work on the disk, without loading it into memory. For some data it was possible to load it into memory using techniques like a bit field to minimize the burden on the memory. Lastly, there were some accounts which were protected, and we could not get data for these accounts. We knew they were in Twitter because we found them, but the access to their data was not granted. We found 1,385 verified users with restricted access to their followers/followings, so we could not get the trusted users respective to them.

11 Conclusion and Future Work

As mentioned previously, this project is a continuation of last year's PFE and is meant to be continued further with an internship at Inria, Sophia Antipolis, under Dr Arnaud Legout. In this project we validated that the trust score is a good metric for quantitatively measuring the subjective notion of trust. We plan to use this in classifying tweets as trustworthy or not. That is the final goal of this work. Vigiglobe (http://vigiglobe.com/v2/) is one of the eighteen companies worldwide having a direct collaboration with Twitter, and they have agreed to share their data with us for this work, which will be used in the planned internship. Without their data, it would not have been possible to have access to the full Twitter stream, because of restrictive access rights. We will start working on it in March 2015.

Bibliography

[1] *Wikipedia article on Twitter.* http://en.wikipedia.org/wiki/Twitter

[2] *About Twitter.* https://about.twitter.com/company

[3] H. Kwak, C. Lee, H. Park, and S. Moon. *What is Twitter, a social network or a news media?* WWW'10, Raleigh, NC, USA, May 2010.

[4] Maksym Gabielkov, Ashwin Rao, and Arnaud Legout. *Studying Social Networks at Scale: Macroscopic Anatomy of the Twitter Social Graph.* ACM SIGMETRICS'14, June 16-20, 2014, Austin, Texas, USA.

[5] Mashable.com. *Eight social media hoaxes you fell for this year*. http://mashable.com/2012/11/05/social-media-hoaxes/

[6] *FAQs about verified accounts.* https://support.twitter.com/articles/119135-faqs-about-verified-accounts

[7] Mashable.com. *Facebook Is Most Popular Social Network for All Ages; LinkedIn Is Second [STUDY]*. http://mashable.com/2011/11/04/facebook-most-popular-forrester/

[8] Maksym Gabielkov, Arnaud Legout. *The Complete Picture of the Twitter Social Graph.* ACM CoNEXT 2012 Student Workshop, Dec 2012, Nice, France.

[9] N. Sharma, S. Ghosh, F. Benevenuto, N. Ganguly, K. P. Gummadi. *Inferring Who-is-Who in the Twitter Social Network*. 4th ACM SIGCOMM Workshop On Social Networks (WOSN), Helsinki, Finland, August 2012.

[10] TechCrunch.com. *Twitter Picked Up 16M Active Users In Q2.* http://techcrunch.com/2014/07/29/twitter-q2-user-growth/

[11] Twitter help center. *Using Twitter lists.* https://support.twitter.com/articles/76460-using-twitter-lists#

[12] Michael Nielsen. *How to crawl a quarter billion webpages in 40 hours*. http://www.michaelnielsen.org/ddi/how-to-crawl-a-quarter-billion-webpages-in-40-hours/

[13] H. Liu, E.-P. Lim, H. W. Lauw, M.-T. Le, A. Sun, J. Srivastava, Y. A. Kim. *Predicting trusts among users of online communities: an epinions case study*. ACM Conference on Electronic Commerce (EC2008), Chicago, 2008.

[14] Y. Matsuo and H. Yamamoto. *Community gravity: measuring bidirectional effects by trust and rating on online social networks*. WWW, 2009.

[15] M. Richardson and P. Domingos. *Mining knowledge sharing sites for viral marketing*. In 8th ACM SIGKDD, 2002

[16] J. Weng, E.-P. Lim, J. Jiang, and Q. He. *Twitterrank: Finding topic-sensitive influential twitterers.* In ACM WSDM, 2010.

[17] D. Ramage, S. Dumais, and D. Liebling. *Characterizing Microblogs with Topic Models.* AAAI Conference on Weblogs and Social Media (ICWSM), 2010.

[18] *About Twitter's suggestions for who to follow.* https://support.twitter.com/articles/227220

[19] D. Kim, Y. Jo, I.-C. Moon, and A. Oh. *Analysis of Twitter Lists as a Potential Source for Discovering Latent Characteristics of Users.* ACM CHI Workshop on Microblogging, 2010.

[20] A. Pal and S. Counts. *Identifying topical authorities in microblogs*. ACM Conference on Web Search and Data Mining, 2011.

[21] Alina Quereilhac, Mathieu Lacage, Claudio Freire, Thierry Turletti, Walid Dabbous. *NEPI: An Integration Framework for Network Experimentation*. Software, Telecommunications and Computer Networks (SoftCOM), 2011.

[22] Simi John. *Morgan Freeman Death Hoax: Bruce Almighty Star Denies Death Rumours.* International Business Times, Oct 2012.

[23] Mashable.com. *Police: Teenage Girl's Viral Tweet Was Kidnapping Hoax.* http://mashable.com/2012/10/01/teenage-girl-tweet-kidnapping/.

[24] Twitter.com. *Rate limits: Chart.* https://dev.twitter.com/rest/public/rate-limits.

[25] *Huffington Post: Eleazar David Melendez.* Twitter stock market hoax draws attention of regulators. http://www.huffingtonpost.com/2013/02/01/twitter-stock-market-hoax_n_2601753.html.