2020-03-16

Identify trust value for fake news detection from a social media

TSEGU, EUAEL

BAHIR DAR UNIVERSITY

BAHIR DAR INSTITUTE OF TECHNOLOGY

SCHOOL OF RESEARCH AND POSTGRADUATE STUDIES

FACULTY OF COMPUTING

Identify trust value for fake news detection from a social media

EUAEL TSEGU HADGU

Bahir Dar, Ethiopia

April, 2019

Identify trust value for fake news detection from a social media

Euael Tsegu Hadgu

A thesis submitted to the school of Research and Graduate Studies of Bahir Dar Institute of Technology, BDU in partial fulfillment of the requirements for the degree of
Master of Science in the Computer Science in the Faculty of Computing.

Advisor Name: Prof. Rama Kirishina Bandaru

Bahir Dar, Ethiopia
May 7, 2019

DECLARATION

I, the undersigned, declare that the thesis comprises my own work. In compliance with internationally accepted practices, I have acknowledged and refereed all materials used in this work. I understand that non-adherence to the principles of academic honesty and integrity, misrepresentation/ fabrication of any idea/data/fact/source will constitute sufficient ground for disciplinary action by the University and can also evoke penal action from the sources which have not been properly cited or acknowledged.

Name of the student EUAEL TSEGU HADGU_______ Signature _______________________

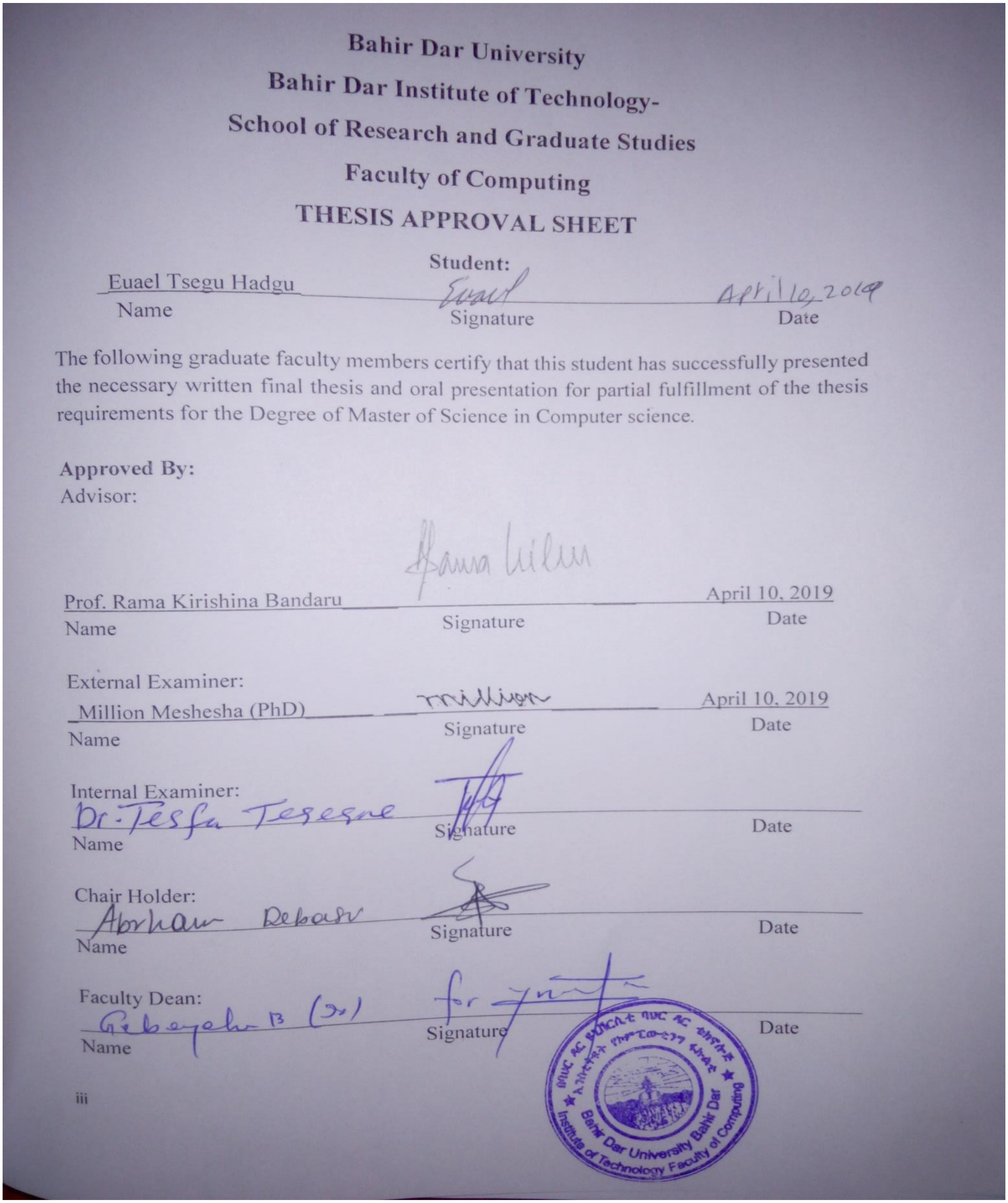
Date of submission: __May 7, 2019______________

Place: Bahir Dar

This thesis has been submitted for examination with my approval as a university advisor.

Advisor Name: Prof. Rama Kirishina Bandaru________________________

Advisor's Signature: ____



Bahir Dar University

Bahir Dar Institute of Technology-

School of Research and Graduate Studies

Faculty of Computing

THESIS APPROVAL SHEET

Student:

Euael Tsegu Hadgu — Euael — April 10, 2019

Name — Signature — Date

The following graduate faculty members certify that this student has successfully presented the necessary written final thesis and oral presentation for partial fulfillment of the thesis requirements for the Degree of Master of Science in Computer science.

Approved By:

Advisor:

Prof. Rama Kirishina Bandaru — — April 10, 2019

Name — Signature — Date

External Examiner:

Million Meshesha (PhD) — million — April 10, 2019

Name — Signature — Date

Internal Examiner:

Dr. Tesfa Tegegne

Name — Signature — Date

Chair Holder:

Abrham Debasu

Name — Signature — Date

Faculty Dean:

Gebeyehu B (Dr) — for

Name — Signature — Date

iii

በባሕር ዳር ዩኒቨርሲቲ ባሕር ዳር ቴክኖሎጂ ኢንስቲትዩት የኮምፒውቲንግ ፋካልቲ ★ Bahir Dar University Bahir Dar Institute of Technology Faculty of Computing ★

To my father and mother

ACKNOWLEDGEMENT

I would like to thank my advisor Prof. Rama Kirishina Bandaru for helping me work on this research and for his continued support during the time of work. I would like to thank the faculty of computing for giving me the chance to learn the Master of Science in Computer Science. Finally, I would like to thank my friends and my mother for their advice and support.

ABSTRACT

Trust analysis on web sources is mostly done using methods like account-based, content-based and activity of the source. In account-based attributes like followers' type, the number of followers, number of likes, type of follows and friends are used to analyze the trustworthiness of the source. When using content-based method attributes like Hashtag (#), includes (@) and links that are found on the post are used to analyze the trustworthiness of the source. When using the activity of the source to analyze its trustworthiness attributes like how many times it posts, the time interval of posts is used. Those methods are useful for posts that are used for marketing purpose adverts or for spammers.

When it comes to real liars, intentionally want to deceive people and hence, it is hard to use those methods for analyzing the trust value of the sources. Because those people try their best, to make their post genuine and they don't make things that makes them look like a spam.

In this research, we are using text content to extract the fact and check if the fact is valued and try to calculate the validity of the facts in order to calculate the trust value of the source. We develop a method that uses sentiment analysis, knowledge base, and a voting system.

The source sentiment to a specific entity is used for calculating the sensationalism of a source to an entity. This is used as a bias in the calculation the trust value of the source with coordination of knowledge base which tries to analyze the past trust value history of the source and the voting system which is used for cross-checking with other sources.

From this research, we were able to get an accuracy of 44.3 % for fake news and 79.3 % for genuine news based on an initial trust value of 0.5. the genuine source accuracy is higher than the fake sources because the genuine sources were small in number but their number of posts were higher than the fake news on the entity Donald Trump, whereas the fake source were large in number but they don't post more than 3 or 4 posts. We observe from the data that fake sources write about diverse topics even though they don't have the knowledge or information. This is why they don't have consistency in their posts.

Keywords: knowledge-base, voting-system, sentiment analysis, social network

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF EQUATIONS

LIST OF ABBREVATIONS

ID	Identification
KBS	Knowledge Base System
NLP	Natural Language Processing
VOIP	Voice over IP

LIST OF SYMBOLS

A(c)	Accuracy of a claim
B	Bias of source
R_e	Reaction of a source to an event
R_o	Change in reaction (opinion) to an entity
S	sentiment value of an event
S_{se}	Sentiment value of a source to an entity
T_n	Trust value of a source at n-pots
T_p	Trust value of a post

CHAPTER ONE
INTRODUCTION

Since its inception, the human race has passed through different eras. In the era of Stone-age man survived by hunting for food, domesticating animals for food and protection and then harnessing animals for farming. Later in the era of Industrial-age, man-built machines to replace manpower and to improve the productivity of food and living standards by several folds. The locomotives and printing machines that were built in this era, gave huge mobility to people, goods and human thoughts. It enabled information to reach more people and far off places.

With the invention of electricity and the contribution of other related innovations for the last several decades, the era of Information-age began 1970's dramatically changing the human lives. In this age of information, we have become highly dependent on the information for our survival. It has affected the economy, politics, relationship, and overall activity.

Even our way of interaction is being changed by information technology. At present time people are preferring email than postal mail, voice over IP (VOIP) than telephone, blogs than newspapers, online shopping than going to market. The reason can be because of its speed, and cost-effectiveness.

The sharing of information among people has built social networks. Our interaction has changed since the creation of social networks. People are using a social network to communicate with friends, colleagues, families. They are also following news about famous peoples, politician, entertainers and other topics using social network media like Facebook, LinkedIn, Twitter, Instagram etc. The social network provides users with microblogging, media sharing and instance messaging tools.

1.1. Background

As of 2018, there are 4 billion worldwide internet users out of which 3.3 billion users are active social network media users. The penetration of the internet has increased drastically with the development of smartphones at an affordable cost to the public (DataReportal, 2018).

Microblogs are blogs that are smaller in size than the traditional blogs and allow to upload images and short videos and are send to a group of people, friends, and coworkers. At present time the use of microblogs as a source of information has increased.

The users of the social network have shown a big increase in the number of users from time to time. The two most famous social networks throughout the world are Facebook and Twitter with several millions of users subscribing.

The figures below show the number of users in Facebook and twitter consecutively from the year 2010-2017. The figures show the number of active users at the end of each year in millions. As shown in Figure 1.1 Facebook has more than 2.19 billion active users and in Figure 1.2 Twitter has more than 336 million active users (Facebook, 2018) (Twitter, 2018).

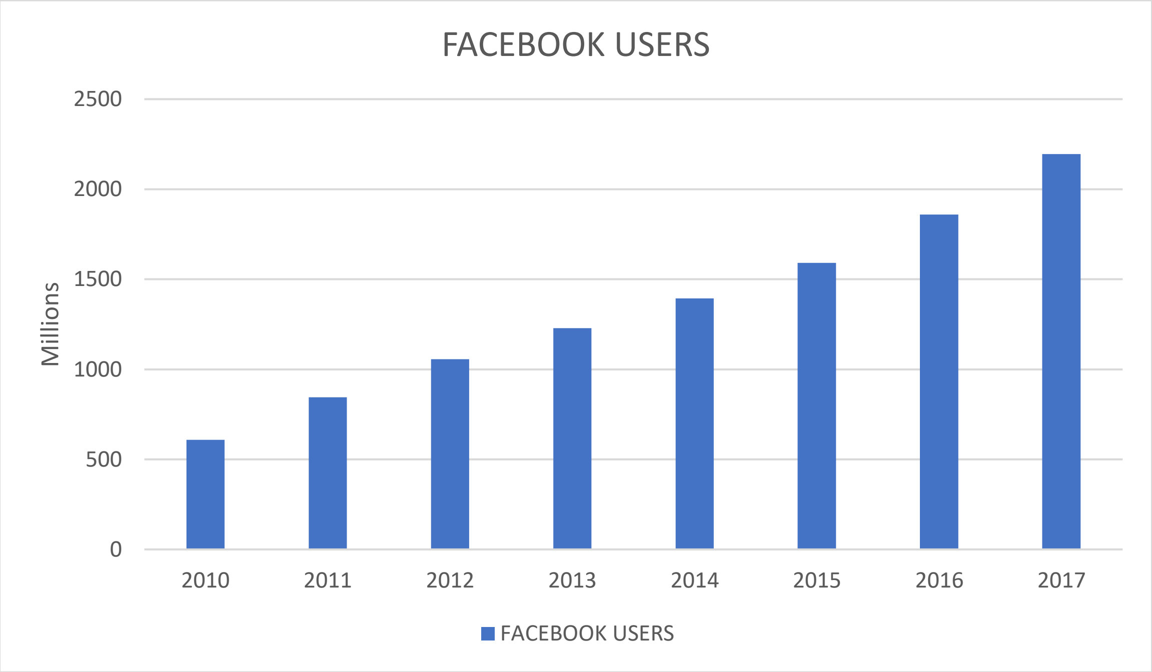


Figure 1.1 Number of active users (in millions) on Facebook (Facebook, 2018)

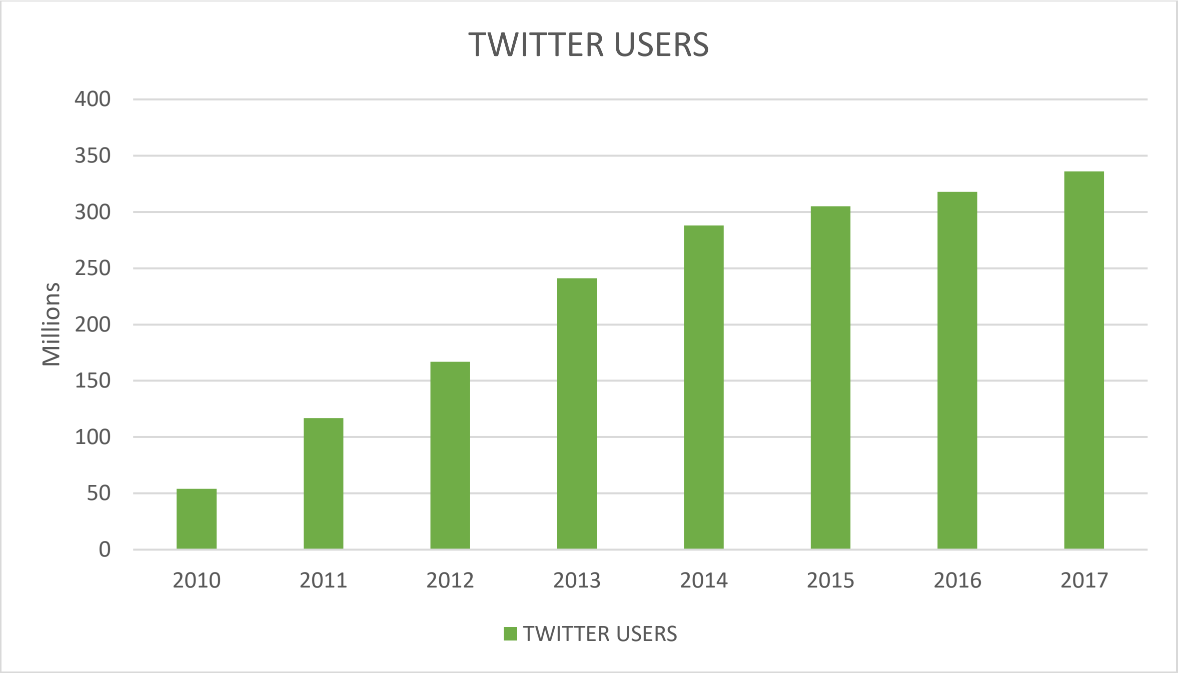


Figure 1.2 Number of active users (in millions) on Twitter (Twitter, 2018)

As compared to traditional media like newspaper, television channel, and radio stations that are run by an institution or organization, blogs are run by individuals. Traditional media go through stages of process and screening to publish an article, but blogs can be written and published within a second without any mediation. So, this makes it less accountable to the information that provides to the audience.

Traditional media has a license to run accorded by organizations or government. And its information is provided after review to make sure it goes with the organization policy and rules. It has ownership of the story that they tell and are responsible for their story. But bloggers don't need any license and it is not ruled by any rules (Hargrove & H Stempel, 2007).

Therefore, the following are certain merits and demerits of using microblog as the source of information (Hargrove & H Stempel, 2007).

Merits:

- The information you get from blogs is real-time and faster than other media outlets.
- One can get information from people which are closer to the story.
- There is little consent in relation to traditional media.

- It is a cheap media outlet for information.
- It doesn’t need any sophisticated equipment or publishing papers.
- It can be done with a mobile phone with internet connection.
- One can cover a worldwide audience.

Demerits:

- The information one gets may be misleading.
- The writer or blogger may not be responsible for the information it posts.
- The writer may not be professional journals or author.
- The information one gets may be offensive and be harassing.

Even though blogs are better than traditional media in many aspects, it is not as credible as the traditional media. One can’t tell which story is correct and which story is wrong, because of the number of blogs written every day, the frequent sharing of information and coping of information between bloggers.

Trust analysis on posts tries to identify, which posts are fake and which posts are genuine. Trust analysis of sources tries to identify the reliability of the source’s information. Trust analysis differs from fake news detection, in that fake news detection try to classify news into two parts fake and genuine. Whereas trust analysis tries to identify fake news by the probability of the news being trustworthy.

To calculate the trustworthiness of a post, trust analysis tries to get all the facts from the post. Check each fact if it is correct or not. It gives the average correctness of the post, So the steps to calculate the trust value of the source is as follow. This is the process of trust analysis (Hamido & Jie, 1987-2017).

- For a given post extract every sentence on the post.
- Check if the sentence is a fact or an opinion.
- If the sentence is fact extract subject, predicate, and object, for example (Barack Obama, born, USA).
- Check if the fact is correct or incorrect.

- Check every fact for correctness give correct fact 1 and incorrect fact 0.
- Get the average of correct facts from all the fact in the post.

The result will be an average number of correct facts on the post over the total number of facts on the post.

- If the average value is 1 the post is 100% genuine.
- If the average value is 0 the post is 100% fake post.
- If the average value is in between 1 and 0, then the post contains correct and incorrect facts.

The need for trust analysis is vital because as this age of information it is difficult to identify if a post is genuine or fake. There are many incidents of fake news becoming viral and misleading. Studies were done on misinformation state that fake news spread faster than genuine news. This study tries to tackle the problem of fake news having a higher audience than genuine news (Hamido & Jie, 1987-2017).

1.2. Statement of the problem

Since it doesn't take any time for a blogger to publish an article, anybody can write information and publish it in web blogs anywhere and anytime, so this makes blogs fast and an up to date source of information. Blogger doesn't need to be a journalist, an expert on the topic or a member of an institute that gives information (media outlets). Because of this, there are millions of articles written every day, and it is hard for anybody to identify which source has correct information and which source has the wrong information.

To calculating the trustworthiness of a post, knowledge base systems use fact checking using cross-checking methods like the voting system and the history of trustworthiness of a source. The problem with the voting system is that fake news can go viral than genuine so the number of fake news will dominate the genuine news. This is because fake news attracts more than genuine news, they affect our feeling more than genuine news (Zhao, Lu, Wang, & Ma, 2015). Knowledge base system depends on the past history of a source to analyze the future posts that the source posts. Both of them don't considering the afflation of the source. If a source is affiliated to a specific entity (country, political group, person, company, religion) it can affect its claims and what it writes about the entity.

The problem with the existing systems is they do not consider the sensationalism of the source. The biases of the source to a specific entity, this entity can be an individual, group of people, state or political party. The sensationalism of a source has a big effect on fact-checking.

It is therefore the aim of this study to incorporate the effect of sentiment analysis on the study of trust analysis of posts written on social media. Studying the sensationalism of a source and its effect on the credibility of the source.

To this end, the current study will attempt to answer the following research questions.

- How much can sentiment affect our judgment and our claim?
- How to use sentiment analysis to check our claim is correct or incorrect?

1.3. Objective of the study

1.3.1. General objective

The main objective of this study is to compute the trust value of a given microblog post from a social media so as to check whether it is genuine or fake.

1.3.2. Specific objectives

To achieve the general objective of the study, this research has formulated the following specific objectives.

- To study and identify suitable methods for trust analysis.
- To prepare the dataset and choose measurement methods.
- To create a method for identifying the sensationalism of a source using sentiment of a source to an entity.
- To design a prototype that detect fake news.
- To evaluate the performance of the prototype.

1.4. Scope and limitation

This study is done for facts that are collected from microblog. The microblogs are collected from social media Twitter and Facebook. We have only taken one entity. That means the microblogs that are collected are written about one entity that is Donald Trump. And the subject of microblogs that we used is about the 2016 USA election.

The data collected for this research is from 14 news outlet source that was reporting news on the election using social media. The facts are crosschecked between those posts. It is very difficult to collect every post that is written about the election from Facebook and Twitter and analyze it to get the trust value. So, we have taken 14 news outlet that is a web-based news outlet and that post their news on the social network.

Because our entity was one. We did not study the relationship between entities. This can have a big influence on the trust value. For example, if we assume that the relationship between the entity Donald Trump and Hilary Clinton is opposite. If a source writes good things about Donald Trump. It may write false claims about Hilary Clinton. So, if we know the relationship between related entities. For entities, we don’t have data we can make assumptions from its relationship with other entities.

1.5. Significance

This research will help people in deciding which source is correct and which source is biased. By showing the trustworthiness of a source, a user can be aware of the truth about the information he/she gets. This will help stop false news and false rumors from going viral.

It will also be used to rank posts on their relevance. Trustworthiness will be used as one attribute to rank posts to be displayed to the user. Two posts having similar information will be placed in order of merit of their trustworthiness. This will improve the ranking process of posts in a social network.

It could be a base-work for other researchers to work on the trustworthiness of the source. It contributes to the current methods of calculation of trustworthiness.

CHAPTER TWO
LITERATURE REVIEW

The big problem with web blogs is that, unlike traditional media, they were not reviewed and analyzed before they were posted (Zhao, Lu, Wang, & Ma, 2015). Every day there are more than 2 million blogs posted. Since these blogs are written by individual users, it is hard to assure its credibility. Microblog users perceive the credibility of their blog based on the metadata and image (video) features which affect the credibility of the source (Byungkyu Kang, 2015).

So how do we check the credibility of those posts which are almost all are written by single users? It is hard to give credibility to a user because of (Byungkyu Kang, 2015):

- They don’t have any duty to write credible source as they are not questioned to take responsibility for their posts.
- They can be anonymous so they may not be known and this will make them write whatever they want.
- Because they write in real time, it is error-prone when posting.

Because of this, people are losing credibility in online media. Survey taken online in United States of America show that the trust level of online media. The survey was done on 1005 respondents. Figures shown below depicts the trust level of different online media with respect to the respondent (Statista, Level of trust in selected online news sources, 2017).

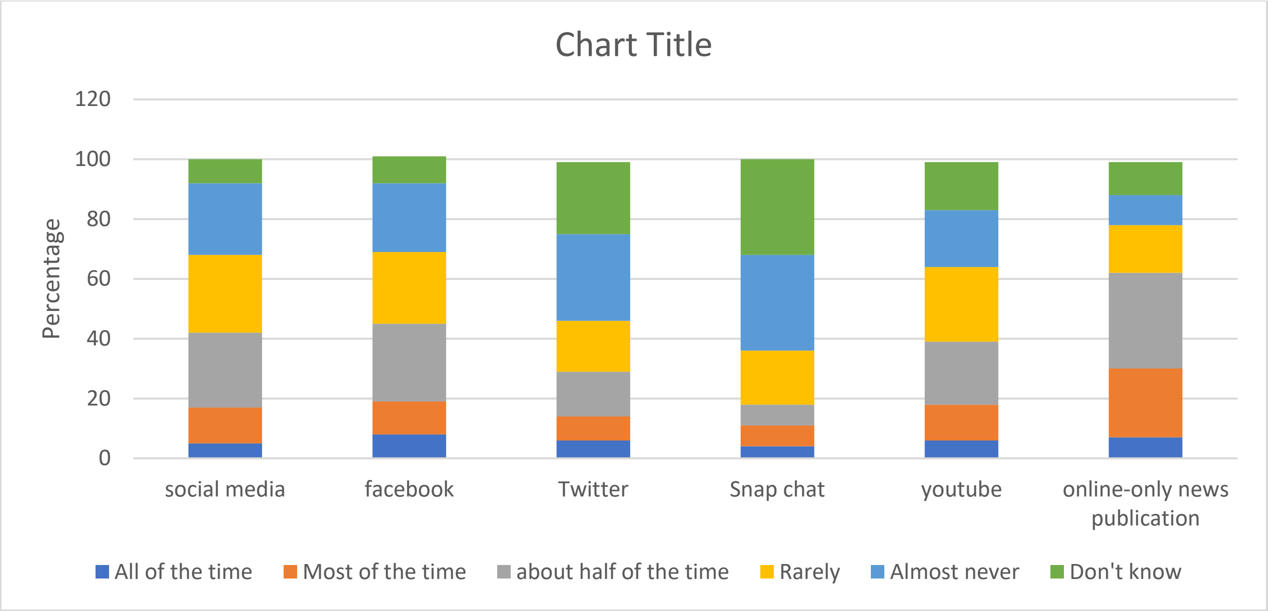


Figure 2.1 Trust value of online media (Statista, Level of trust in selected online news sources, 2017).

Some of the figures are not 100 % because of rounding of the numbers. On another survey which was done on 803 respondents. Show the frequency of fake news seen on online media. Figure 2.2 shows the percentage of a fake news report (Statista, Perceived frequency of online news websites reporting fake news stories in the United States, 2018).

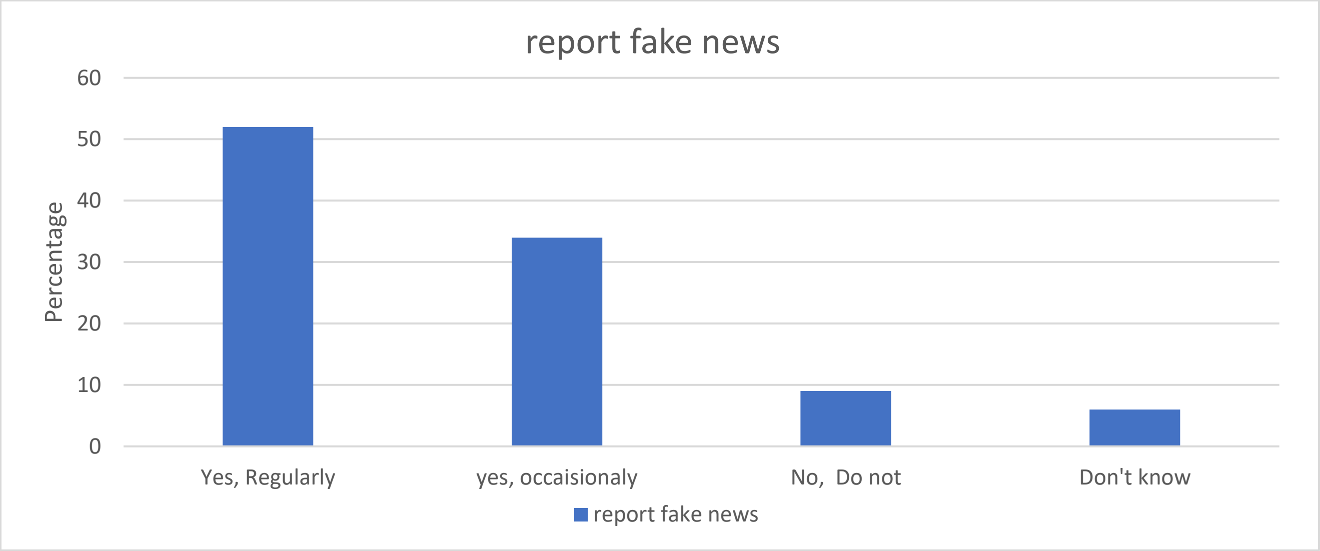


Figure 2.2 Report of fake news (Statista, Perceived frequency of online news websites reporting fake news stories in the United States, 2018).

2.1. Fake news

In traditional media, the content consumer was very large and the content creator was a small group of institutions. The institutions or organizations was owning what it says it was accountable for what has been claimed.

So, in traditional media, they hire a professional journalist to create content. After that, there are fact finders who checks the truthfulness of the content created. Then it is reviewed by editorial if it could be published. The content must obey the policy and rules of the institution. Thus, in the traditional media, it has many processes to publish a piece of article.

But now a day with the creation of social media everybody is the content consumer as well as the content creator. Everybody has the freedom to write what they want. As the traditional media, it will not force to own its claims. So, this makes it less credible. Because timing is essential in news the traditional media are becoming less popular and people are going to blogs. After reading the specific news it is quite unlikely to cross-check with other media.

Fake news has greater number of sharing and viewers than the actual news. There have been many studies that report that fake news has high rate of acceptance than correct news. The research done by (Soroush, Deb, & Sinan, 2018) used twitter posted from 2006 to 2017 by 3 million users and 126,000 rumors. The rumors were represented as a cascade, in such a way that one rumor can be represented as having an origin and number of retweets as one cascade. And the cascade was quantified with the following attribute depth (number of retweets), size (number of users interacted in the cascade), maximum breadth (the maximum number of users interacted with a single retweet) and structural virality (the size of content spreading).

From this research they were able to find out that false news reaches 1500 users 6 times faster than true news and genuine news takes 20 times longer to be retweeted 10 times than false news. Politics and urban legends go viral than other kind of news. Finally, false news was likely spread 70 % faster than true news.

The reason for this was the dramatic effect of false news and the inside story effect of the news. It was found that false news has more dramatic or novel kind of writing than the fact, this get the attention of listeners. The inside story effect is that the story was written from someone who have been closely involved in the story. This was the second effect that make false news preferable than the truth. They have the inside story effect than the truth (Soroush, Deb, & Sinan, 2018).

Some of the reasons why people are misinformed are (Sandra, Rebecca, & Anna, 2017):

I. Self-selection bias

People interact with similar minded people which make them ignore who have different ideas or claims. The information they get will be from a group of people who have the same opinion as theirs. So, their knowledge is biased on those groups claim. This will make their judgment biased on one side.

II. Crowd psychology

People are inclined to run when they see a crowed running. People will have a big tendency to retweet a certain claim if it has been retweeted by many others.

III. Social identity theory and Conformity

People tend to retweet an article in order to show that they are part of a group. To tell they belong to a certain group. As a way of confirmation, they are a member of a certain group. Even though they don’t agree with what been written.

IV. Trusting family and friends

People tend to believe their families and friends and they don’t check the original source of the information. They tend to validate who posted and don’t bother to check from which source was originated

V. Credibility noise

People retweet or share information without reading the content by only reading the headline and viewing an image or video. Most people are affected by content production technologies (like Photoshop and alike photo editors). The content production technology creates a credibility noise that will make the content more credible.

Effect of misinformation

- Misallocation of resource in terror attacks and natural disasters.
- Affect Business investments.
- Misinformation in elections.
- Devalues and delegitimizes voices of expertise, authorities, and institutions.
- The financial cost of exposing and elimination a fake news.

2.2. Web spam

Spams are unwanted messages and posts that are used communicated with malicious websites for the purpose of advertisement, phishing, virus distribution and other criminal purposes. There has been increasing use of spams on the social network. There have been millions of spam accounts on social networks like Twitter and Facebook. And there have been many mechanisms to identify spam accounts and spam posts in a social network.

Spams use luring mechanism like (Soroush, Deb, & Sinan, 2018)

- Using hot issues and sensitive topics in their headlining in order to get hits.
- By promising to provide free software, game, books etc.
- By photo editing and presenting it as genuine.
- Following many users in order to get many follow backs which will make them popular and trustworthy.

There are different mechanisms for identifying spams on a social network (Liu, Wang, Zhang, Chen, & Xiang, 2017). There has been a lot of research on spam detection. For the detection of spam in social networks, they used different features one is content-based, which try to analyze the content of the tweet. It used to analyze if the tweet has links (HTTP), hashtags (#) and includes (@). Almost all spams have links by which they use the victim to lure to their malicious website. They have many hashtags to get many audiences especially popular hashtags. They also include users so that they can get an audience from the user's followers. By using a hashtag, they increase the number of audiences. So, this was used to identify if an account was a spam or not (Miller, Dickinson, Deitrick, Hu, & HaiWang, 2014).

Another method of spam detection was by using a time interval of tweets and the age of the account. By analyzing the time interval between twitters, it can be identified if an account is a spam. Because spammers tweet frequently. If the time window between tweets is small it can be a spam. Spam accounts don't stay online for long as time goes their popularity decrease because people will notice them and they will be detected by the social network and closed so most of the spams have young age compared to legitimate accounts (Jeong, Noh, Oh, & Kim, 2016).

Spam detection mechanism that uses both content-based and account-based detection. In content-based they use the number of hashtags, number of retweets, number of usernames mentioned, number of digits in a tweet, number of characters in tweet and number of links, and the account-based use number of followers, number of followings, number of likes and account age (Liu, Wang, Zhang, Chen, & Xiang, 2017).

Another method of spam detection using the similarity of friends between accounts. That is, we can identify if an account has a similar friend with the friends or the people, he/she follows.

For spam detection, those methods are useful because those features can identify if an account is a spam or a legitimate account. They use the characteristics of spam to detect the spammers.

But for fact checking it is difficult to use spam detection techniques because in the fact-checking the outliers don't change too many accounts, they don't add friends from different groups they target specific group, they are not reported as spam so they will not be placed in the spam blacklist, they have a specific topic of discussion every time. This makes them difficult to identify them as spam detection methods.

2.3. Data integration

Data integration is the process of creating a combined data which is collected from different heterogeneous sources, to create a unified data that can have one view for all of the sources. For example, student information of all Ethiopian university to have one access, integrating patient information of every hospital in Ethiopia.

In data integration, data are collected from different sources. So, they will have different data representation. To make them easily accessible the different data representation is converted into universal data schema. The data is then checked for duplication. Then after duplication is checked there will be the process of data fusion. Data fusion is used to create a single consistency and accurate data which represent a real-world entity.

Data integration can be as simple as two tables joining using union or join instructions and it can be very complex such that data integration for creating a knowledge base from the web source.

When data is integrated it need to be complete, concise and correct. Completeness means the amount of data, which it is represented in entities. In order to make a data integration complete, we have to increase the sources of data as much as possible. Conciseness means there is no duplication of data representation. This is done by deleting redundant data and merging attributes of a data that have the same entity. Whereas correctness means the data must be accurate and consistent. The correctness of data is done by data fusion.

2.3.1. Data fusion

Data fusion is used to resolve a conflict between data. Conflict can be uncertainty and contradiction. Uncertainty means one or more sources having null value where others have value for specific data of single value. Whereas contradiction means having different values from different sources for single-valued data. Single value data means having a single value for a data. For example, the sex of Abebe this can be only female or male one of the two (Xin Luna & Felix, Data Fusion – Resolving Data Conflicts for Integration, 2009).

Conflict of data can be resolved by one of those three methods.

Conflict ignoring: In conflict ignoring they don't know if a conflict has occurred, hence they will not resolve the conflict.

Conflict avoidance: In this method they know there is conflict but they don't resolve them individually.

Conflict resolving: In this method try to resolve each conflict that occurred. They try to resolve the conflict based the freshness of the data or reliability of the source.

The accuracy of a source is used to check the reliability of the source this can be done by statistical analysis of the source. The freshness of the data can be checked by the timestamp of the data (JENS & FELIX, 2009).

The contradiction may occur not only because of having contradiction but by some other factors such as (JENS & FELIX, 2009):

- Out of date data, which this may create conflict if the data don't have a time stamp in it. For example, if in a source that was updated 2009 says that MR. X is 29 years old and another source that was updated in 2010 says that MR.X is 30 years old. They both are correct but if we don't have the time stamp (updated time) this can create conflict.
- Data owners may not want to give access to their data or they may not want their data to be merged with other data. Real-time data fusion can be difficult with the creation of millions of data from different sources. It will be hard to obtain and process all the data.

Data fusion can be used to create a knowledge base (Xin Luna, et al., 2014).

2.3.2. Knowledge base

The knowledge base is a collection of information or knowledge stored about a specific topic on some kind of library (storage). It is a source of information for the specific topic like a library. The knowledge base is mostly used with knowledge base systems like expert systems.

Knowledge base system (KBS) is a system that uses knowledge to reason, solve-problem, learn and make decisions. Knowledge base system has a knowledge base, interface, and inference engine. The knowledge base is as we explained a set of information, an interface by which a user can communicate with the system and inference engine is a system that creates new information from the given information. For example, k1= Abebe is a father of Belay k2=Belay is the brother of Tola. If k1 and k2 are in our knowledge base, then our inference engine can create knowledge like this k3=Abebe is the father Tola.

Knowledge base systems are used for customer service, help desk and for an expert system. KBS help company to interact with the customer without the need to of hiring an employee. It will reduce the staff that needs for customer service and help desk. This is very important for companies that have millions of customers. There may be a thousand people looking for information at any given time about the company service or asking for help. KBS is also used for expert systems. Expert system is a computer program that simulates an expert human being like doctor, lawyer, nurse, etc. the program will act as an expert and people will interact with the system as it interacts with the expert.

So, for creating KBS we need knowledge base and most of the knowledge base build for KBS are built manually. Many knowledge bases that have large general knowledge facts like Freebase, Wikidata, YAGO, NELL, Deepdive, etc. are built manually some of them by company others by collaborative users (Xin Luna, et al., 2014).

Data integration methods can help to build a knowledge base. From which we can check if the information is correct or incorrect. For example, if we want to check if Ethiopia is found in Africa or Asia. We create information library or knowledge base for new information that is uploaded on the web. We will not need for someone to update our knowledge base manually. But to make a knowledge base built artificially it needs many things like checking if the information is correct. Correctness in terms of extraction correctness and source correctness.

2.4. Sentiment analysis

A sentiment is having some kind of feeling like anger, sadness, happiness, scared etc. a feeling can create emotions that can cause someone to react to psychological or physical change. Emotions are related to behavior. Some people can be very emotional relative to others for the same reason can act differently. Sentiment can affect our action. It can change our behavior from the way normal we behave or act.

Sentiment analysis is the process of analyzing the sentiment of a text, speech or other document using natural language processing, machine learning, and other biometric methods. Sentiment analysis extracts, process and quantify the type of sentiment. Sentiment analysis can be a polarity checker which identify if the sentiment is positive or negative or to more complex sentiment analysis that can identify feeling like anger, happy, sad, grief, love, etc. Sentiment analysis can help extract information about specific users view, opinion and attitude by his text and reaction the web (V.Mäntyl, Graziotin, & Kuutila, 2017).

In recent years there have been many applications of sentiment in different area like business, politics, healthcare, etc. many companies are looking to sentiment analysis to gather information about their customers. By using rating, comment, and social media posts to extract the sentiment of the users about product performance. Big companies are using sentiment to find out if a new product has a positive or negative feedback from the users. Rating and like this can tell us the general feeling of the user on the product. Comments and posts about the product can tell specific features of the product which the users like and which features they dislike. By mining the opinion of the users, the companies can make an improvement on those things that the users did not like (Usman, AL-KHARUSI, & Awwalu, 2015).

There has been an influence of sentiment analysis in an election and political polls. Collecting posts and microblogs from social media to know the feeling of the people and manipulate this information to gain votes (Anuta, Churchin, & Luo, 2017).

It is also used to choose adverts based on the persons likes or feelings. It is also used to identify if the content of the web contains offensive or sensitive content. And try to warn if it is suitable for users or if it is age appropriate for children. It can also try to identify if someone is having some kind of psychological problem. And try to warn before he/she becomes suicidal.

Sentiment analysis can be done on document, sentence or feature word. Document-level sentiment analysis analyzes a set of sentences as a whole to get the feeling of the document as positive or negative. In document-level sentiment analysis, it works well if the sentiment is about a single entity. Sentence level analysis tries to analysis a sentence it first tries to identify if the sentence is feeling (subjective) or fact (objective). Then if the sentence is subjective (feeling) it calculates its sentimental value. Word level sentiment analysis try to identify all the sentiment words in a document or sentence and to what it is impaling (D'Andrea, Ferri, Grifoni, & Guzzo, 2015).

Sentiment analysis can be done using machine language or using a lexicon. Machine language use methods like a k-nearest neighbor, Naïve Bayes, neural network tools to identify the sentiment by training in leveled data. In the lexicon, the method used a sentiment dictionary to identify the sentiment words and calculate the sentiment of the document or sentence (Barretto & Morajkar, 2017).

There are also other tools that use symbols (emoji) on a document to identify the sentiment of a document like an emoticon. Septic net is also another tool that uses semantic analysis to identify the sentiment of a document. Some tools like EWGA (entropy-weighted genetic algorithm) use a genetic algorithm to identify the sentiment of the document (Barretto & Morajkar, 2017).

Rule-based sentiment analysis, in this method for a given document, each sentence is extracted. From each sentence, the part of speech of the words is tagged. By using rule, the sentence is classified if the sentence is objective or subjective. And if it is subjective its words are given sentiment value and the final sentiment value of the sentence is calculated (Collomb, Costea, Joyeux, Hasan, & Brunie, 2013).

Another method is using lexicon based it gives value for any sentimental words. And gives features for the supervised machine learning algorithm. The algorithm creates a feature vector which sums up the sentiment value or calculates the number of occurrences. To give the feeling of the text.

There are methods that used a probabilistic calculation of the sentiment of sentences that are used on products that use the sentiment calculation of a sentence in relation to its rating of the product. Given a product rating 1-5 the user can give the rating. Using this rating to cooperate with its comment on the product to find the sentiment value of the comment.

2.5. Related works

Trust analysis is the processes of analyzing the trustworthiness of a source. There are many factors to analyze in order to find the trustworthiness of a source. For a giving source s: s ∈ S where S is the set of all sources. For a claim c: c ∈ C where C is the set of claims about a specific fact. We can calculate if the claim is correct (probability of being correct) and we can calculate the trustworthiness of the source by calculating the probability of all its claims.

Research done by Jeff Pasternack & Dan Roth (2011) on generalized fact-finding uses 4 attributes to calculate the trustworthy of a source and the believability of the fact. It uses a three-layer graph with weighted values on the edge of the graph to calculate the believability of the fact and the trustworthy of the source. To calculate the weights of the graph it uses 4 factors that affect the trustworthy of the source.

Uncertainty on the extraction of the source that tells us about the certainty that claim c was found in source s. There may be an extraction error. How much is the extraction error probability? This will affect the believability value because the error may not be from the source but from the extraction.

The uncertainty of the source about the claim, this shows that how certain is the source about its claims. For example, “I am 90% sure … “this will affect the believability value because the source only believes in it 90% of the time.

Group membership, a source can be a member of one or more groups. So, it is inclined to have the same claim as its group. For example, if one is a member of BBC news employee it will agree with the claims of other members in the institution. This is will affect the trustworthy of the source.

Research done by members of Google on trust analysis (Xin Luna, et al., 2015), they created a model that tries to calculate the accuracy of the source based on the source accuracy and the extraction tool accuracy. They claim that the extraction error is more error-prone than that of the source. So, to decrease the error of the extraction it uses different extraction tools.

By extracting triple containing a subject, a predicate, and an object from a source. Where the subject is an entity in the real world and the predicate is an attribute and the object the value of the attribute for the entity. It deals with how to estimate the trust value (accuracy) of a source for every triple it gives.

It takes into assumption that the triple is a single-valued triple. For example. the nationality of Abebe (Abebe, nationality, Ethiopia). Some triple may not be single-valued like Abebe's child. For computational speed, they ignored multi-value triples.

The idea is by using the redundancy of the internet to find out the accuracy of a source. Or the trustiness of a source. But not by neglecting the error of an extraction. So, they built a 3-dimensional model that calculates the accuracy of the source by using a set of extractors and web sources data and value. They take into consideration when calculating the accuracy of the source the extractors' extraction accuracy and the previous trust value of the source. (Xin Luna, et al., 2015)

Fake news is more viral than genuine news. So, this will affect the believability of a genuine news from fake news. Because fake news is spread faster than genuine news it is believed more than the genuine news. So, this will affect voting system to find if a news is fake or genuine. Because fake news is written in a way, they can get the attention and feeling of user by adding false information (Sandra, Rebecca, & Anna, 2017).

Previous done works on trust analysis, they don't consider the effect of sentiment of a source on the things it writes. A source can be bias to things it is affiliated. So, when the source writes about those things. It can affect its writing or it can be bias. For example, a Donald Trump supporter can be bias when writing about Donald Trump or Hilary Clinton. Using the previous works this kind of bias is not taken into consideration. So, in this research we are taking into consideration the effect of the sentiment of an entity in calculate the biasness of a source. And use this bias to calculate the trust value of a source.

CHAPTER THREE
METHODOLOGY

3.1. Overview

This research aims to create a framework that calculates the trust value of a source and the trust value of a claim. This research uses empirical and probability-based data analysis to create a model. In order to build the framework. The main component for the trust analysis is sentiment analysis and data fusion. To create the framework, we have studied the relationship between sentiment and trust value, and proposed a method by which we can integrate sentiment analysis with data fusion to calculate the trust value of a source and claim. Figure 3.1 below shows the process followed to accomplish this study.

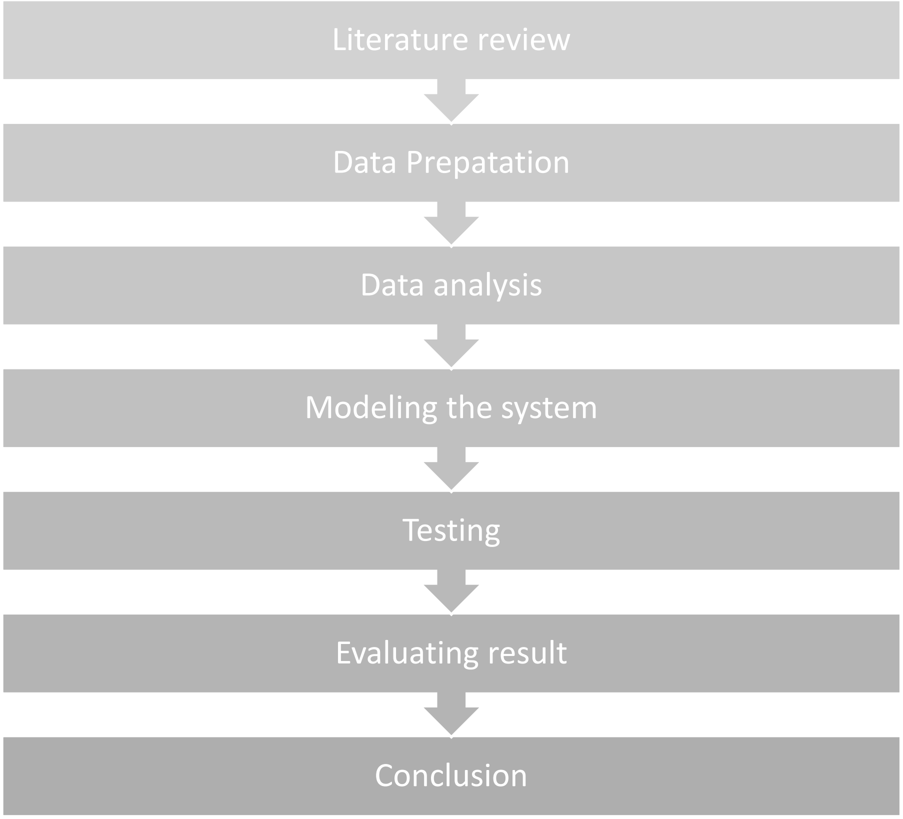


Figure 3.1 Research process

3.2. Dataset preparation

The dataset for trust analysis is available from various sources such as: from journalists, from crowdsourcing like Wikipedia and from individuals. The problem of the dataset for trust analysis is that the data should be labeled as trustworthy or untrustworthy. To do this one has to crosscheck a claim, go to authorities to check for the truth or gather evidence to check the truth. To label one claim may take many hours of work. Because of this, we are forced to analyze the existing free datasets which is better for us than to collect our own dataset. Different datasets are available for researches on fake news detection like BuzzFeed News (Silverman, Shaban, Singer, & Strapagiel, 2016), "Liar, Liar Pants on Fire" (Wang & Yang, 2017), BS Detector (Shu, Sliva, Wang, Tang, & Liu, 2017), CREDBANK (Mitra, Tanushree, & Gilbert, 2015), and Fake News Net (Shu, Sliva, Wang, Tang, & Liu, 2017). Fake news detection is checking whether a given news has actually happened or it is made up.

CREDBANK is fake news dataset which gathered from Twitter from October 2014 to February 2015. It contains 169 million tweets, 62,000 topics, and 1300 events. Event topics where given credibility value. The credibility values are -2 (Certainly Inaccurate), -1 (Probably Inaccurate), 0 (Uncertain or Doubtful), +1 (Probably Accurate) and +2 (Certainly Accurate). Credibility value was calculated using 30 different Amazon Mechanical Turk. This is computer machines that perform jobs of an expert system for different tasks choosing a picture for a product, price determination, description writing, quality management etc. (Mitra, Tanushree, & Gilbert, 2015).

Liar, Liar Pants on Fire: is dataset which is collected from radio, television, newspaper, and websites. The dataset is a collection of data from interviews, speech, comments, and news. It contains more than 12,000 labeled sentences. The short sentences are manually labeled by a human (Wang & Yang, 2017).

Fake News Net: this includes 240 labeled sentences dataset from news websites that were posted on Facebook and Twitter from their website. Its dataset contains both social content and news content. And has equal size of genuine news and fake news (Shu, Sliva, Wang, Tang, & Liu, 2017).

BuzzFeed News: this data was collected from Facebook posts by 9 news outlet the news outlets where from rightwing, leftwing and mainstream. It contains more than 1000 posts that are labeled as mixed of true and false, mostly false, mostly true and no factual content (Silverman, Shaban, Singer, & Strapagiel, 2016).

BS Detector: this dataset which is collected from a web browser plugin app that rate posts credibility by analyzing links, that are found on the posts to find if the link is reliable or not reliable from manually labeled domains (Shu, Sliva, Wang, Tang, & Liu, 2017).

From the above datasets, we choose Fake News Net. BS detector and CREDBANK where labeled by computer so the result, we get will be in comparison to those algorithms that analyzed the labeling of the data. Buzzfeed news dataset is a good one but it has very few false news in comparison to the true news. The ratio of true to false news is 16:1, this will make the data analysis biased to the truest news. And Liar, Liar panties on fire most of the data are audio interviews. It is not similar to the written news that a person writes intentionally to mislead. So, we have decided to go with Fake News Net because of its content have 480 labeled true and false news, that are posted in a social network on Facebook and Twitter, and has much news related to Donald Trump this can help as build sentiment relation between the source and Donald Trump (entity) for data analysis.

3.3. Trust analysis Architecture

When we want to check the validity of an information, we cross-check with another source, or we may choose a certain credible source of information from their past history. We may also choose affiliated (biased) source that can improve judgment of the claim. In this research, we are using those 3 main variables to check the validity of a source or a claim.

The main ideas for our trust analysis are:

- Presuming that the most posted claim has the highest trust value.
- Presuming that if the source in the past has given incorrect information in the past, it is probable that it will give incorrect information again. Similarly, if the source in the past has given correct information, it will give correct information in the present also
- Presuming that if a source is biased, that it might give incorrect information.

In order to use these premises, we have to use different pieces of knowledge like:

- Sentiment analysis to analyze the biases of a source to a certain entity.

- To use the history of a source to analyze the future, we have to use a prediction method.
- To analyze the most claimed source we have to use probability method.

This research uses sentiment analysis, data fusion and machine learning methods. The model of the trust analysis model using sentiment is as follow: -

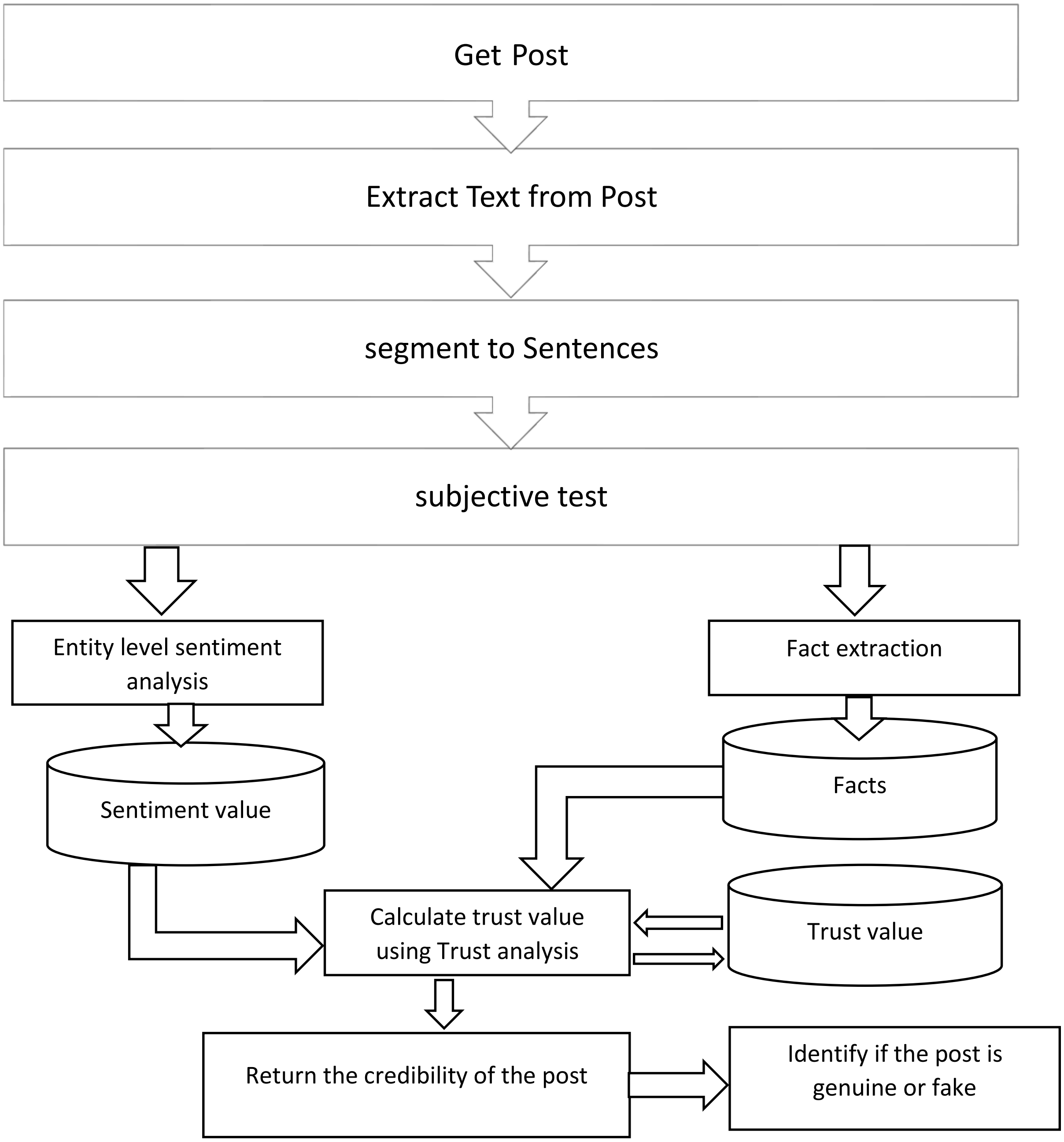

Get Post
Extract Text from Post
segment to Sentences
subjective test
Entity level sentiment analysis
Fact extraction
Sentiment value
Facts
Calculate trust value using Trust analysis
Trust value
Return the credibility of the post
Identify if the post is genuine or fake

Figure 3.2 Architecture of trust analysis

- For a given post, we extract text by eliminating noises like links, pictures, and videos.
- After getting the text. We segment the given text into sentences.
- For every sentence, the subjective value is calculated and every sentence is classified into subjective and objective. Subjective having *sentiment* and objective having *fact*.
- For the subjective sentences, the sentiment value of the source to an entity is calculated and stored. In this, the stored data will have source *ID, post ID*, *entity name* and *sentiment value*.
  - Source ID is the unique identifier used to identify each source. A source is anybody who use social media to give information or news.
  - Post ID is a unique identifier given to each post that is written by the source.
  - Entity name is any subject that is talked about in the post. It can be a person, country, group of people, thing, situation etc.
  - Sentiment value is the sentiment of the source to the entity which he is writing about.
- For the objective sentences, we will extract the fact which contains object, predicate and subject and store with source id and post id. The subject and predicate will be used to search the object. Where the object will be used as a value that we can check (Thangavel, 2018) (Studyandexam, 2018).
- We calculate the trust value of the post and the new trust value of the sources. We use the subject as the entity for sentiment value extraction from the sources. The trust value of a source will have source id, trust value and post id.

Finally, we give trust value for every post at a given time by using sentiment value, previous trust value, and extraction value.

3.4. Used tools

To analyze the data python programming language was used. Python is chosen because it is powerful, simple and has good libraries for math processing. Some NLP packages like Text-Blob and ‘Vender Sentiment’ for natural language processing are used. Text-Blob was used for tokenization and for subjective analysis. ‘Vader Sentiment’ was used for sentiment analysis. Stanford Core NLP was used for data extraction.

3.5. Sentiment analysis

Sentiment analysis is the process of language analysis for extracting and measuring the feeling of the data. It is used in many areas to get the opinion of the population. In this research, we are using sentiment analysis to find out the biases of a source. If a source has a feeling for a specific subject. The information is provided about the subject may be biased. It may be exaggerated or not true.

So, in this research, we have use sentiment analysis to identify if there is bias between the source and its information. Sentiment analysis has created the relationship between the source and the subject that it is writing on. And try to create if it has a relationship between the sentiment and the credibility of the source.

When we analyze the sentiment of a source and its information, we want to extract polarity value such as positive, negative or neutral feeling to the subject. In this research, we want to know if a source has a positive or negative feeling about the subject and if this can affect its judgment. We use Vader Sentiment to analyze the sentiment of the source to the text it posted (Gilbert & Hutto, 2015).

Vader Sentiment is rule-based sentiment analysis which uses measured lexical features and measured lexicon dictionary. It uses machine learning methods like support vector machine, Naïve Bayes and Maximum Entropy. It also considers the common acronym (Lol, BF) and slang languages (Nah, giggle) and finds synonymy for them.

The reason why Vader sentiment was chosen was (Gilbert & Hutto, 2015): -

a) The research was done for microblogs.
b) It has high accuracy in relation to other sentiment analysis from data that was collected from Twitter, Amazon, movie review and New York time editorial as shown in the figure.
c) It can analyze different topic data, like politics, entertainment, product review
d) It has fast performance. This is good when analyzing big data.

For a given source, we calculate the source to entity relation for every post and every entity that is in every post. In every post the source publishes, if any entity exists the sentiment is calculated. Every sentiment value has 3 identification those are the source, entity, and post.

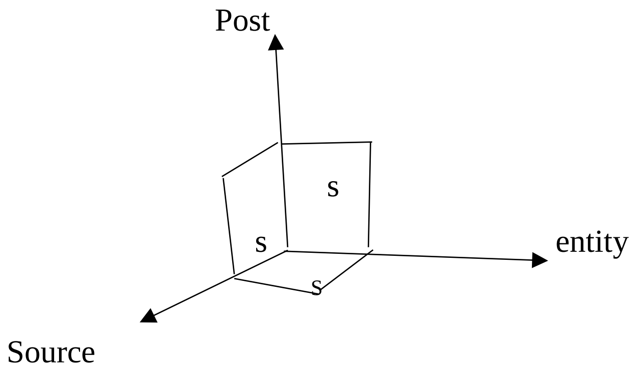


Figure 3.3 source, entity and post relation to sentiment (S)

To calculate the sentiment value of source to the entity at a given time. We calculate the addition of every sentiment value related to the post. So, this cumulative sentiment will be used in calculation the trust value of the source. This will be used as the bias that is created by the source.

To calculate the cumulative sentiment value of the source and the entity we add up every sentiment value of the source to the entity. In here for every subjective sentence that is related to the entity, we extract the entity-based sentiment of the source. For web post, we get the ***sentiment value*** of entity.

$$S_{s\grave{o}}^{n} = \frac{\sum_{i=0}^{n-1} S_{s\grave{o}}^{i}}{n} \quad \text{……………..} \ (3.1)$$

Where **$S_{s\epsilon}$ is the sentiment of the source** in relation to an entity, *n* is the nth- post of the source at which the entity is present and *n* starts from 0. In the nth-post of the sentiment of a source to an entity is found by adding the sentiment of the source to an entity of all its posts divided by *n*. In here if the source has *m* posts then $n \leq m$.

Data fusion: is a consistent and accurate data. Data fusion is used to create a unified data that can be used to create information. Most of the time data fusion is used in sensor data integration.

Voting theory: is the theory that the claim with the highest vouch has the highest accuracy. For a given claim ‘c’ member of a set of claims C= {} where c ∈ C, if claim c has highest vouched in the number of sources it is used as an accurate data (Urken & Arnold, 2011).

For example, if C= {c_1, c_2, c_3} for sources with claims from C, if c_1 was extracted from 2 sources, c_2 was extracted from 3 sources and c_3 was extracted from 5 sources. So, claims c1, c2 and c3 will have an accuracy of 0.2, 0.3 and 0.5. This is calculated using the probability function. From this c_3 is more accurate than c_1 and c_2, and c_2 is more accurate than c_1.

$$A(C_k)= \frac{\sum_{s_i \in S} f(s_i, c_k)}{\sum_{s_i \in S} \sum_{c_j \in C} f(s_i, c_j)} \quad \ldots\ldots\ldots\ldots\ldots\ldots (3.2)$$

$$f(s, c) = \begin{cases} 0 & : \text{if c not found in s} \\ 1 & : \text{if c found in s} \end{cases}$$

Where, A(c_k) is the accuracy of a claim, s is source and c is claim that are found from the source. s є S and c є C (s and c are elements of a set S and C respectively). *f* (s, c) is a function that returns 1 if claim c is found in source s and 0 if claim c is not found in source s.

In a voting system, we consider that: -

- The data must be unique that means duplicates are eliminated. For example, shared data, retweeted tweet or reposted post is eliminated.
- The data must be single-valued data. It shouldn’t be multiple value data. For example, Mr. x is 20 years old. This is single value because age can have only one value.

- Whereas Mr. x is the brother of Mr. y¸ in which Mr. x can have many brothers so this one is multiple value claim.
- In here the extraction or acquiring of the data is assumed to be 100% accurate. It means the extraction error or transmission error is not taken into consideration.
- A source can only provide only one value.
- A source must be consistency.
- A source may not say that Mr. x is 20 years old and Mr. x is 21 years old at the same time.
- Extraction Time variant value must be taken into consideration, if source s1 says that Mr. x is 20 years old in the year 2011 and source s2 says that Mr. x is 22 years old in the year 2012.

The problem with the voting system: -

i. All sources may not have equal reliability so given all sources, equal confidence will create an incorrect result.

ii. Some data may be slightly modified from others sources. This will increase the accuracy value.

iii. In social media, the rate at which false data spread is greater than that of genuine data. This will affect the accuracy (Soroush, Deb, & Sinan, 2018).

iv. Claims that are acquired from unstructured data has extraction error. This will affect the accuracy value.

For these reasons, it is not reliable to consider only the voting system for data fusion or accuracy rating of claims that are extracted from non-structured data and unknown sources. So, it has to be incorporated into other methods to analyze the accuracy of a source. This may work well for a structured data with a reliable source but not on the web.

Knowledge based system

Knowledge-based system (KBS) is a system or model that use past knowledge in its decision making. KBS is mostly used on expert systems. They analyze the past history when solving problems (Hamido & Jie, 1987-2017).

In data fusion, we can use past information to predict the probable future. If a source was accurate in the past, it is most probably be accurate in the future. Similarly, if a source was inaccurate in the past it is most probably be inaccurate in the future. To use past knowledge in predicting the future we can use probability function. The trust value of a source T lies between $1 \leq T \leq 0$. To calculate the trust value of a source T*n*.

$$T_n = \frac{\sum_{i=0}^{n-1} T_P^i}{n} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.3)$$

T_n is the ***trust value*** of a source at the nth post. It is calculated by adding all the trust value of the source in every post dividing by the number of posts until the nth. Initial probability of a source's trust can be given from empirical data analysis. This can be used with the voting model to analyze the trust value of a source.

3.6. Using knowledge to calculate accuracy

In order to get the accuracy of a claim and the trust value of a source, we can combine above two models. The idea is to have different confidence values to the sources. The confidence value is the measurement of reliability of a source. By combining equation 3.2 and Tn trust value of a source. We get: -

$$A(c_k) = \frac{\sum_{s_i \in S} f(s_i, c_k) T_n^i}{\sum_{s_i \in S} \sum_{c_j \in C} f(s_i, c_j) T_n^i} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.4)$$

When we replace Tn with equation 3.3. we get: -

$$\mathrm{A(c_k)}= \frac{\sum_{s_i \in S} f(s_i, c_k) \frac{\sum_{i=0}^{n-1} T_i}{n}}{\sum_{s_i \in S} \sum_{c_j \in C} f(s_i, c_j) \frac{\sum_{i=0}^{n-1} T_i}{n}} \quad \text{……………... (3.5)}$$

Our confidence in the source is dependent on the knowledge of the source, being trustworthy or not? This will eliminate giving equal value to a reliable source and to an unreliable source.

Here we calculated the accuracy of a claim by combining the *voting system* and the *knowledge-based* (Equation 3.2 and Equation 3.3). T_n is used as the confidence value (reliability) of the source to its claim. This accuracy of a claim c_k ($A(c_k)$) is calculated using the trust value of a source at the nth post.

Until now, we were seeing on a specific claim but one post can have multiple mutually exclusive claims. To calculate the trust value of the post we have to add up all those claims that are on the post.

$$\mathrm{T_p}= \frac{\sum_{i=0}^{n-1} A(c_i)}{n} \quad \text{……………... (3.6)}$$

Where n is the number of claims on a specific post. And T_p is the trust value of the post or the accuracy of all the claims on a single post.

To calculate the trust value of a source: -

$$\mathrm{T_n}= \frac{\sum_{i=o}^{n-1} T_p^i}{n} \quad \text{……………... (3.7)}$$

When we replace trust value of the post (T_p). we get: -

$$T_n = \frac{\sum_{i=o}^{n-1} \frac{\sum_{i=0}^{m-1} A(c_i)}{m}}{n} \text{ ……………... (3.8)}$$

This will be the new trust value of the source T_n. In the new trust value of the source is calculated by the addition trust value all of the post written by the source divided by the number of posts that has written.

3.7. Using sentiment in calculating the Trust value

Media has been used to transfer information to the public. Most of the information they broadcast is current information like news. Most of the news providing media concentrate on politics and social issues. Same groups use media to transfer their ideology. This makes those media to be biased toward one group or ideology. Media can be biased in such:

- Criticizing or praising specific group unequally or excessively.
- Missing out news or giving little coverage to the news.
- Exaggerating information to give wrong information.
- Writing false news to mislead the audience.

From the above, the most common kind of bias is criticizing or praising overly and exaggerating information (Jeong, Noh, Oh, & Kim, 2016).

Media biases (sensationalism) is created with a difference in ideology, a difference in opinion and having an unbalanced feeling. All of this led to the creation of sentiment to a specific ideology, group or specific person (Shu, Sliva, Wang, Tang, & Liu, 2017).

In this research, we want to create a model that can use sentiment analysis to create trust analysis of a source that in cooperates the source sentiment relation to the information it gives. We try to quantify sentiment value based on the use of unbalanced reaction to event and change in opinion about a specific entity.

To analyze the unbalanced reaction to an event we use the difference in mean deviation of the source reaction and the overall standard deviation reaction.

For a given event from the source's information we analyze the sentiment of the event the sentiment value is rated from -1 to 1. -1 being absolute negative and 1 being absolute positive. To make relative sentiment with others we normalize the sentiment value to 0 being absolute negative and 1 being absolute positive.

The reaction value is the difference in reaction between sources that cover a specific event. For every source we estimate the sentiment value for the event then we calculate the reaction value of a source to an event using the mean deviation and standard deviation.

For an event, there can be the difference in reaction from different sources. To evaluate the reaction of a source to an event, we calculate the difference between the mean deviation of the source and the standard deviation of the population.

$$\mathrm{R_e} = \sqrt{(s_s - \bar{s})^2} - \left(\sqrt{\frac{\sum_{i=0}^{n-1}(s_i - \bar{s})^2}{n}}\right) \quad \text{……………... (3.9)}$$

$\mathrm{R_e}$ is the reaction of a source to an event. $\mathrm{S_s}$ is the sentiment value of the source and $\bar{s}$ is the mean sentiment of sources to an event. $\mathrm{S_i}$ is the sentiment value of source i. n is the number of sources on which has posted on the event. In here we are assuming that in a single post there will be one event.

Another reaction we have to take is the opinion change. To find out if there is an opinion change between the source and the entity in its writing on. This is the difference between the sentiment of the source and the entities between its posts.

$$R_o = \frac{\sum_{j=0}^{m-1} \sqrt{(s_{sj} - \bar{s})^2} - \sqrt{\frac{\sum_{i=0}^{n-1} (s_{ij} - \bar{s})^2}{n}}}{m} \text{ ……………... (3.10)}$$

R_o is the representation of the change in opinion on the entities. S_{sj} is the sentiment value of the entity j to the source s which is calculated on equation 3.1. This is done for all the entities that are found on the event or post. This change in opinion is compared with other sources. In here we have m entities and n number of sources. For all the entities that are found in the post we are calculating the change in reaction of every source by using mean deviation and standard deviation.

To calculate the biases of a source we take the average reaction of event and change on reaction of the source to entity.

$$B = \frac{R_e + R_o}{2} \text{ ……………... (3.11)}$$

When we replace R and R from equation 3.7 and equation 3.8. We get: -

$$B = \frac{\sqrt{(s_s - \bar{s})^2} - \left(\sqrt{\frac{\sum_{i=0}^{n-1} (s_i - \bar{s})^2}{n}}\right) + \frac{\sum_{j=0}^{m-1} \sqrt{(s_{sj} - \bar{s})^2} - \sqrt{\frac{\sum_{i=0}^{n-1} (s_{ij} - \bar{s})^2}{n}}}{m}}{2} \text{ ……………... (3.12)}$$

Those reaction value will be used to calculate the biases of a news outlet to the entity and will be used in the calculation of the trust value of the source and a post.

$$T_p = (1\text{-B})\frac{\sum_{i=0}^{n-1} A(c_i)}{n} \quad \text{……………... (3.13)}$$

The biases of the source affect the accuracy of the post. If a sources' biases equal to 0 it will have no effect on the accuracy value of the post by the source. But if the source has biases it will affect the accuracy value of the post. The biases affect the accuracy of the post by 1-B.

$$T_n = \frac{\sum_{i=o}^{n-1} T_p^i}{n} \quad \text{……………... (3.14)}$$

When we replace T_p with equation 3.1, we get; -

$$T_n = \frac{\sum_{i=o}^{n-1} (1-B)\frac{\sum_{i=0}^{m-1} A(c_i)}{m}}{n} \quad \text{……………... (3.15)}$$

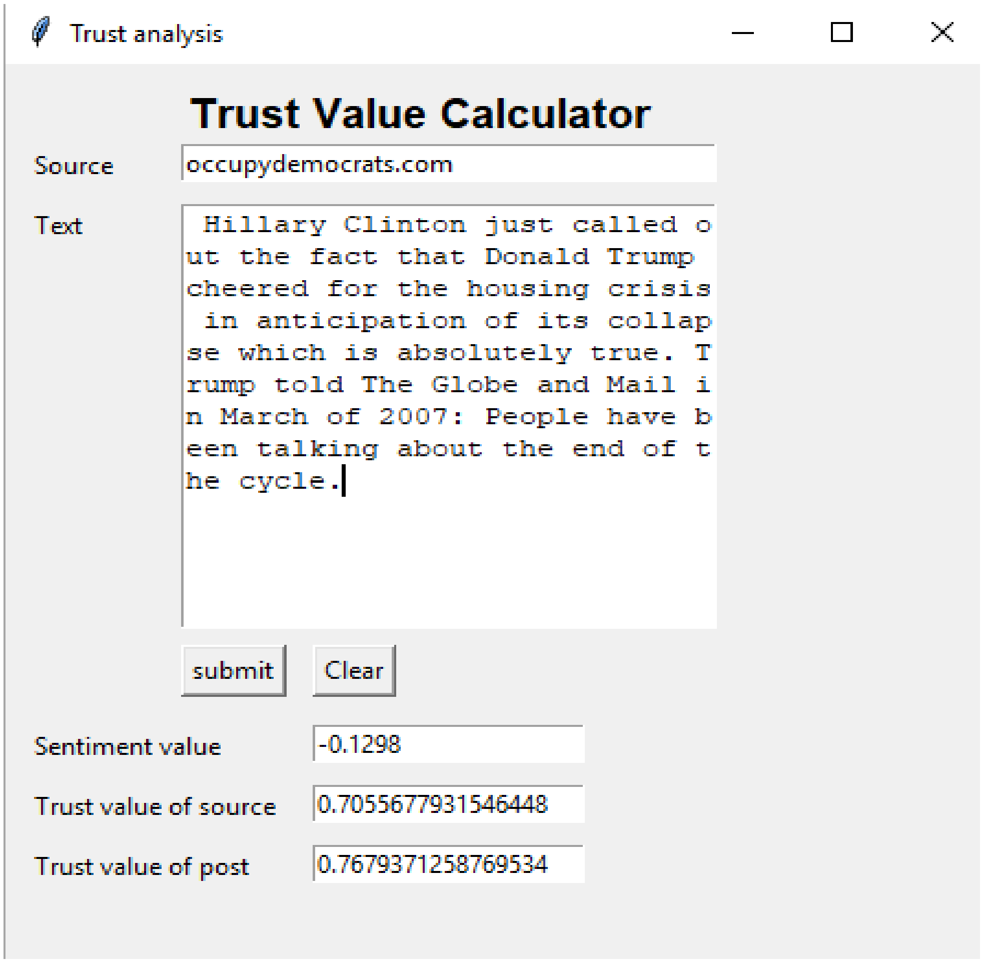
This will be the trust value that use B as the coefficient of bias which is created by the sentiment value. Sentiment bias will have an indirect relation to trust value.

3.8. User interface prototype for analyzing trust

The prototype will accept the name of the source and the post that the source has written on the text box. After accepting this the prototype will return the sentiment value of the source, trust value of the post and trust value of the source. To get those result the following steps are performed.

- First, it will calculate the sentiment value of the text.

- It will segment the text into sentences. Check if the sentences are claims or opinion.
- If a sentence is a claim. Get the entity (subject) of the sentence.
- From the knowledge base get sentiment value and trust value of the source in relation to the entity.
- Calculate the trust value of the sentence. Go to step 3 and do for every sentence on the text.
- Calculate the average trust value of every sentence. This will be the trust value of the post.
- Using the calculated trust value of the post and from the knowledge base every trust values of the posts that the source has written. calculate new trust value of a source.



Trust Value Calculator

Source occupydemocrats.com

Text

```
 Hillary Clinton just called o
ut the fact that Donald Trump
cheered for the housing crisis
 in anticipation of its collap
se which is absolutely true. T
rump told The Globe and Mail i
n March of 2007: People have b
een talking about the end of t
he cycle.
```

Sentiment value -0.1298

Trust value of source 0.7055677931546448

Trust value of post 0.7679371258769534

Figure 3.4 User interface for calculating the trust value of a given post

As shown in figure 3.4 after inserting the source and the post in the text area. We click submit and the system will calculate the sentiment value, trust value of the source and trust value of the post. Three of the values are stored in the knowledge base. For the next trust value calculation.

The final output of the prototype is the sentiment value of the text, trust value of the source and trust value of the post. The sentiment value as shown in Figure 3.4 it has -0.129 value. This means that the post has a negative sentiment. The trust value of the post has 0.755677. This indicates that the post has 7 out of 10 claims are true and 3 claims are false. The trust value of the source is 0.7679. This means that the source claims 7 true and 3 false out of 10 claims he/she make.

CHAPTER FOUR
RESULTS AND DISCUSSION

4.1. Data set description

The dataset contains 233 posts which are posted on Facebook and Twitter by websites providing news. From this data set, we have chosen 95 posts that talk about Donald Trump. We choose Donald Trump because it was the highest written entity as compared to other entities. From these 95 posts, we have 65 sources. From those sources, we have to choose sources that posted more than one times in order to see the effect of our method.

For a genuine news we had 9 sources and for fake news we had 5 sources. in combination, we had 14 sources out of the 65 sources. From the genuine news we had 53 posts and from the fake sources, we had 13 posts. The table below shows a number of sources and their corresponding posts and type of post.

Number of sources	Number of posts	Type
2	2	Fake
3	3	Fake
1	2	Genuine
2	3	Genuine
2	4	Genuine
1	6	Genuine
1	7	Genuine
1	10	Genuine
1	14	Genuine

Table 4.1 number of sources to their corresponding number of posts

As shown in the table number of genuine news are more than those of fake news. This show that writes fake news to have inconsistency in their posts and write about different entities. There is no news source that has both genuine and fake news at the same time in our data set.

4.2. Experimentation

When experimenting we have to take the different parts of the method into consideration and know their effect. These are the voting system, the knowledge base, and the sentiment part. Depending on our data we have to take some things into consideration.

The method as written in chapter 3 has different parts. For a given post to calculate the trust value of its post, it has to extract every fact from the post. Each fact contains a triple: subject object and predicate. This will be used to cross-check with other sources triples. In order to check the probability claim. Since our data contains small posts, we could not find similar triples. We could only find 3 triples which were claims by less than 3 sources. This is because of the time gap of the data was posted.

We gave all the posts equal 1.0 value for their voting value. It means that their claim belongs to them, and no other source that claimed it, which makes sources not sharing the trust value. This will also allow us to eliminate the error which was occurred in extraction.

In knowledge base system, future trust values depend on the previous posts trust values. When a source writes its first post. We have to give it initial trust value to the source in order to calculate the trust value of the source at any given post. In this research we have given them different values for experimenting like 0.01 assuming first he/she is a liar (all his/her claim is false), a value 0.99 means he/she is trustworthy (all his/her claim is true), and 0.5 means that he/she has equal number of true claim and false claim. But we recommend that it should have an empirical value which is observed data from different sources and use it as an initial value.

To analyze the sentiment, we have to analyze the different sentiment values and their effect on the trust value of the source. These are the change in reaction on an entity R_o, reaction to an event R_e and the bias B of the source which is the average of the change in reaction and the reaction to an event.

We define error rate as difference between correct fact whose value is 1 and the incorrect fact whose value is 0. We analyze error rate by calculating the trust value using those sentimental reactions.

4.3. Reaction to an event

An *event* is any situation that happened in a given time. This can affect the sentiment value of the source to the entity and make their post biased. Because our data was posted sparsely, we could not find specific events that can be used for analyzing the reaction of a source to an event. So, we take into consideration in a given time T there will be a set of events that are done by some entity. For the given data at a time T, we calculated the reaction to the set of events that are done by the entity. A source will have an effect on its post by the effect of events that are done by an entity.

Each line on the figure is a source that wrote about an event on the 2016 USA election related to the entity Donald Trump with the number of posts they have written about the election.

Inhere as the number of posts of a source increase the accuracy of the system on the prediction of the trustworthiness increase. An error is an absolute value of the real trustworthy value (for genuine is 1 and for fake is 0) subtracted from calculated trust value.

So as the number of posts from each source increases the error value is decreasing. This show that the system we are using is improving its accuracy as the number of posts increase. It can identify with less error if the source is genuine or fake as the number of posts written by a source increase.

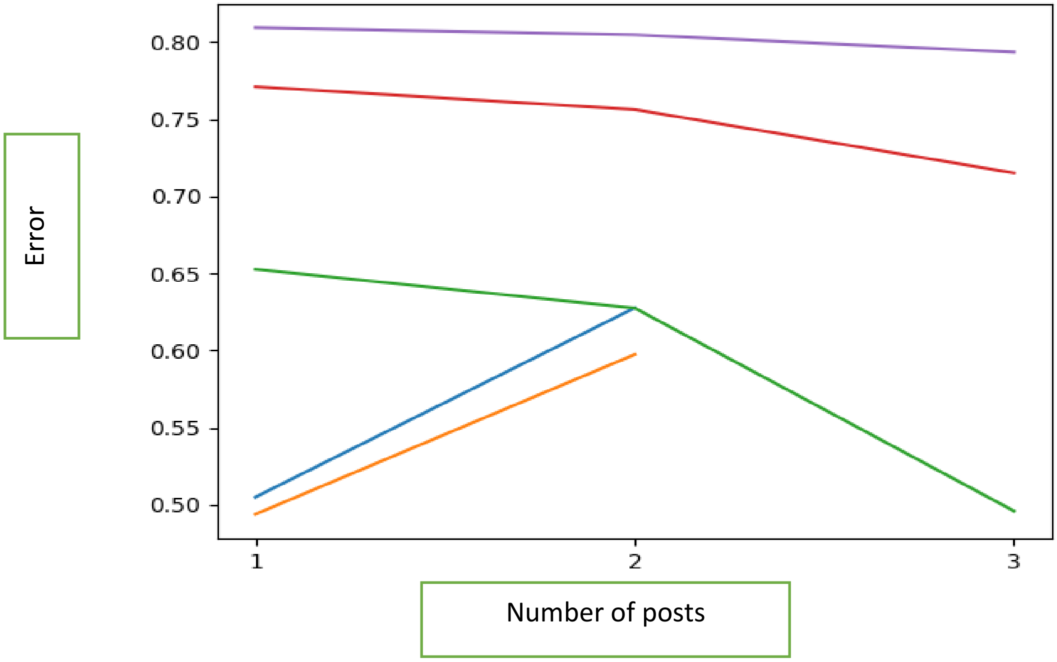


Figure 4.1 error value of trust for a fake source calculated using event reaction (Re) for a given initial trust value of 0.01

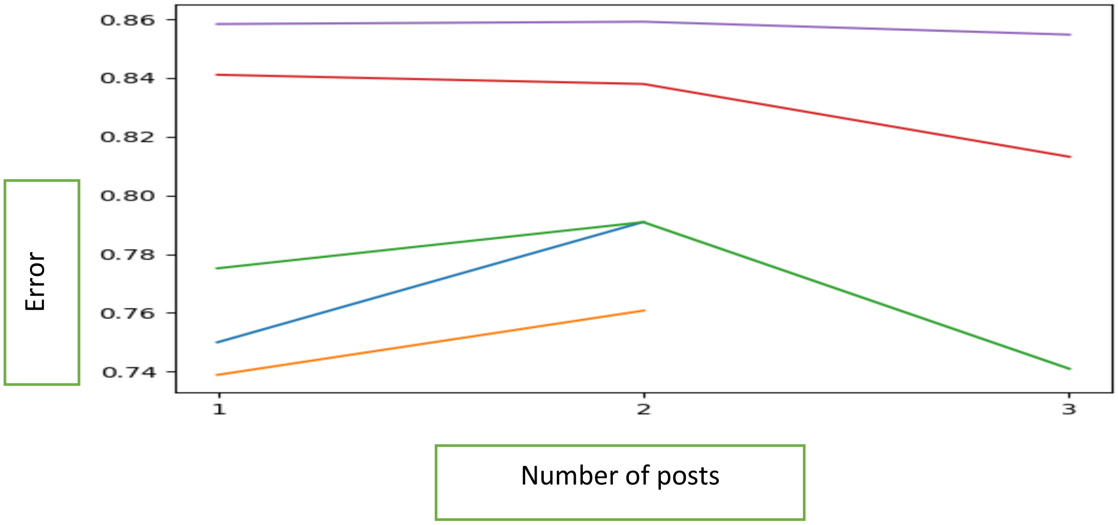


Figure 4.2 error value of trust for a fake source calculated using event reaction (Re) for a given

initial trust value of 0.5

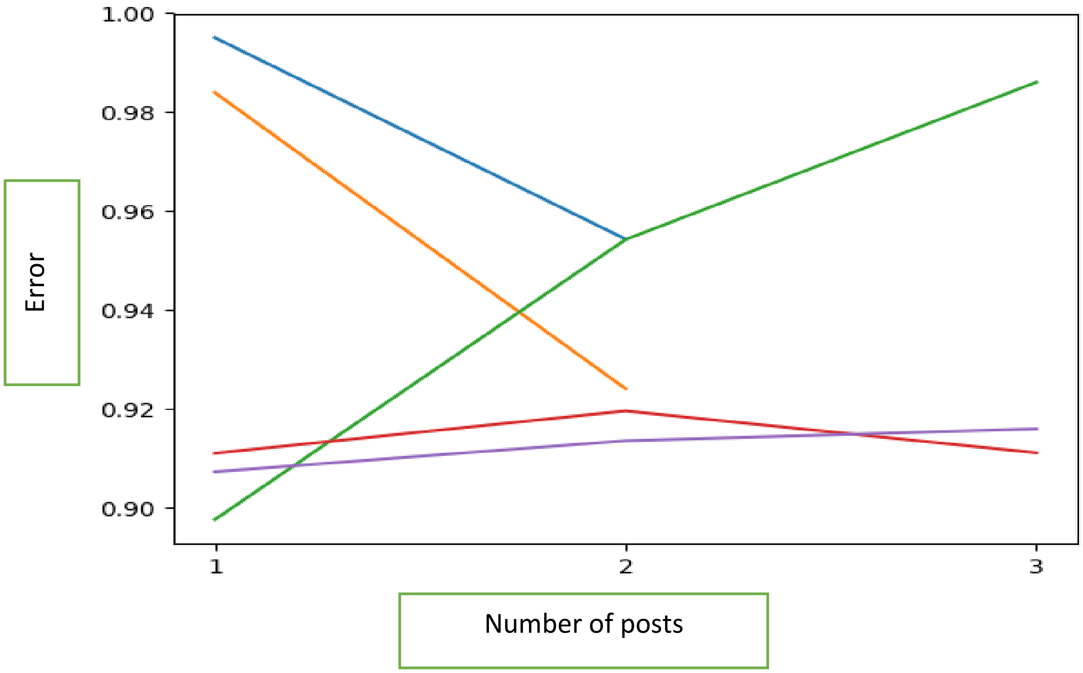


Figure 4.3 Error value of trust for a fake source calculated using event reaction (Re) for a given initial trust value of 0.99

Figure 4.1, 4.2 and 4.3 show fake news error values. Figure 4.1 has lower error value compared to Figure 4.2 and Figure 4.3 because Figure 4.1 has an initial trust value of 0.01 which is closer to 0 than to 1. So, this makes it closer to false. In Figure 4.1 we are assuming all sources are fake. So, the error rate is much lesser than Figure 4.2 and Figure 4.3.

The error value in Figure 4.3 is greater than Figure 4.1 and Figure 4.2. In Figure 4.3 we have given the source initial trust value of 0.99 which is closer to 1, which means we are assuming every source is genuine. This will affect the calculation of trust value. Because the sources are all fake the error value has increased than that of in Figure 4.1 and 4.2.

As shown in figures, for sources that have 3 posts had shown a decline in the error value as the number of posts increase. This is because of the knowledge base system, which uses the trust value of the past in the calculation of the future it makes the error value decrease. But the sources with 2 posts, the error value has increased especially when their initial value is closed to their future values. This is because their reaction to the event has increased that their error value also increased.

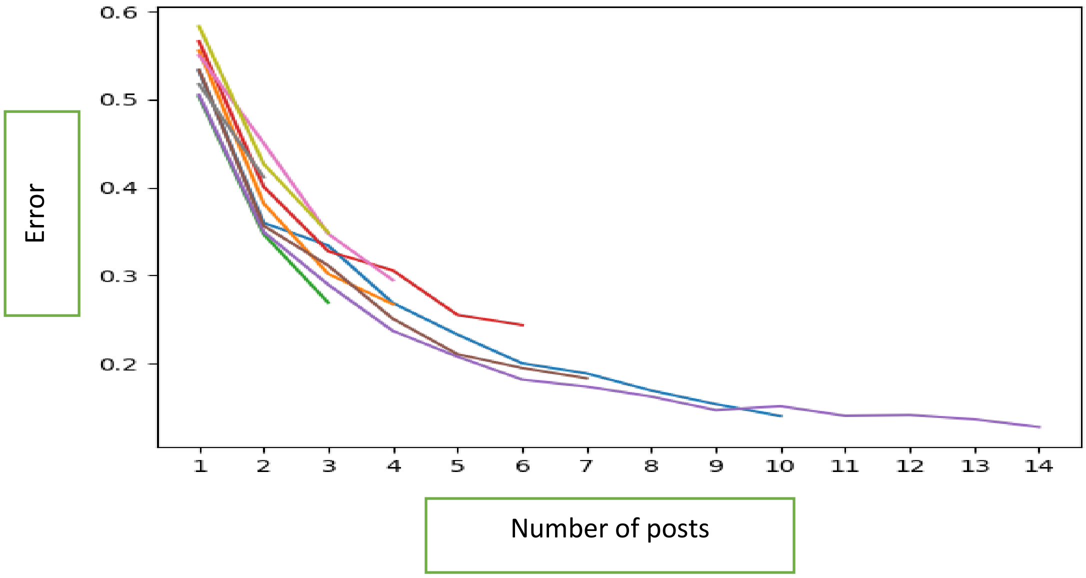


Figure 4.4 error value of trust for a genuine source calculated using event reaction (Re) for a given initial trust value of 0.01

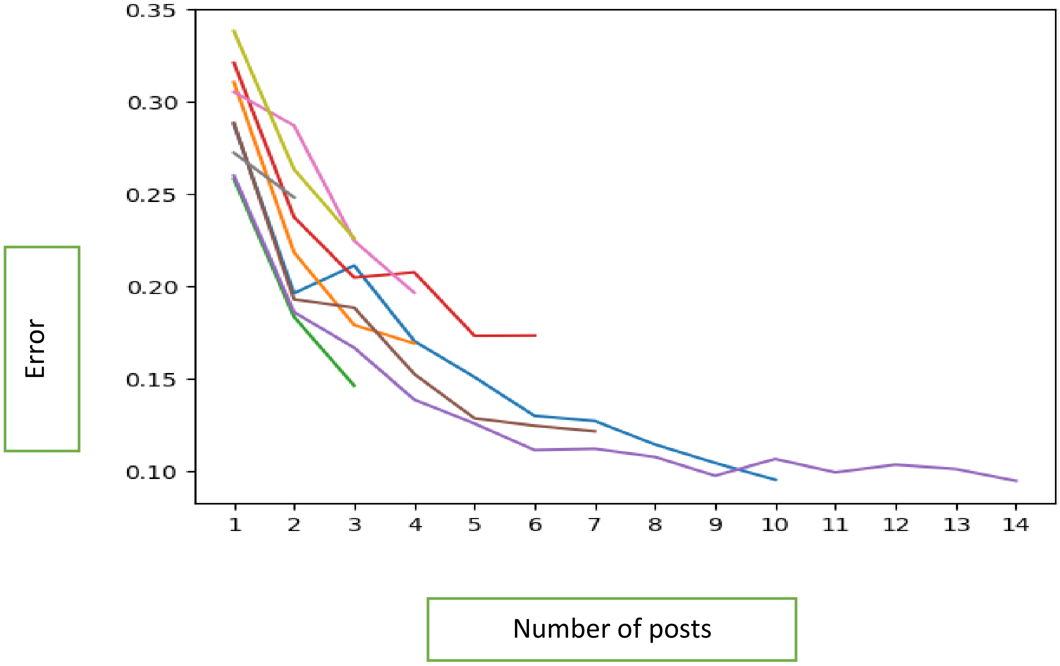


Figure 4.5 error value of trust for a genuine source calculated using event reaction (Re) for a given initial trust value of 0.5

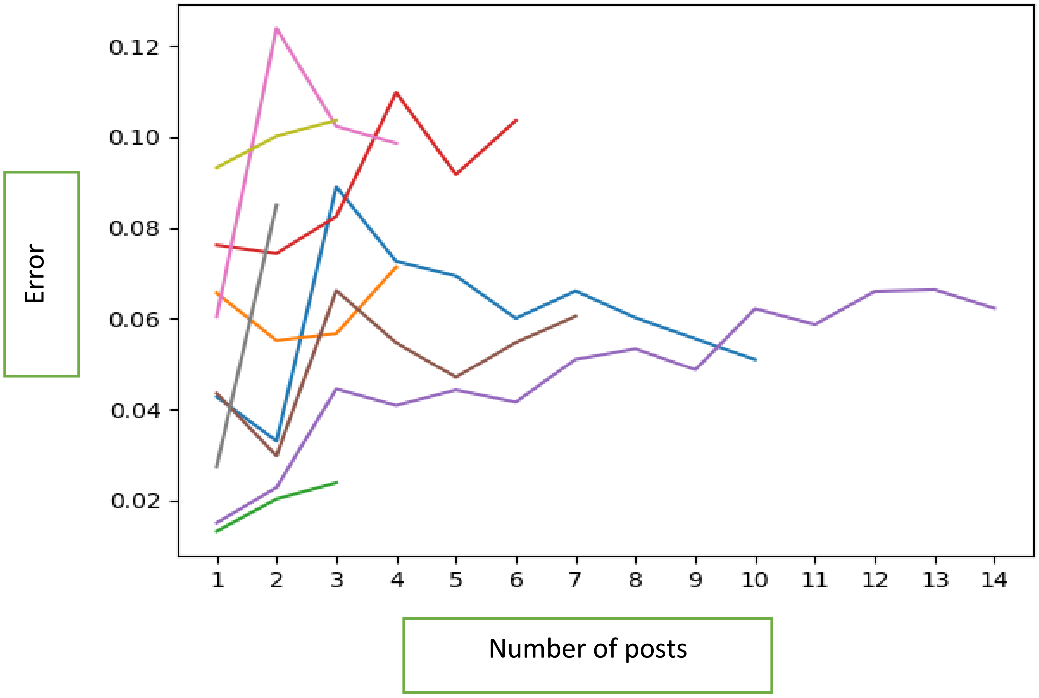


Figure 4.6 error value of trust for a genuine source calculated using event reaction (Re) for a given initial trust value of 0.99

As shown in Figure 4.4 it has higher error value compared to Figure 4.5 and Figure 4.6. This is because in Figure 4.4 we are assuming initially all sources are fake. This will make its error value greater than the others figures. As we can see in Figure 4.5 it has an error value smaller than that of Figure 4.4 and larger than of Figure 4.6. This is because of the initial value we have given it is 0.5 so this makes greater in value than that of Figure 4.6.

In Figure 4.6, error value increases to some points then it is declines gradually. This is because we have given the initial trust value 0.99 which almost have a true value. So, this makes it have little error value at start given all the sources are genuine. It will have its effect until 2 to 3 posts.

4.4. Change in opinion about an entity

In here we will calculate the change in the reaction of a source to an entity. If the source changes its attitude to an entity it will have an effect on the things it writes about the person. We will try to analyze the change in the reaction of a source to an entity. This will be used to calculate the trust value of the source. In Figure 4.7, it is shown the error value of a source at a given post.

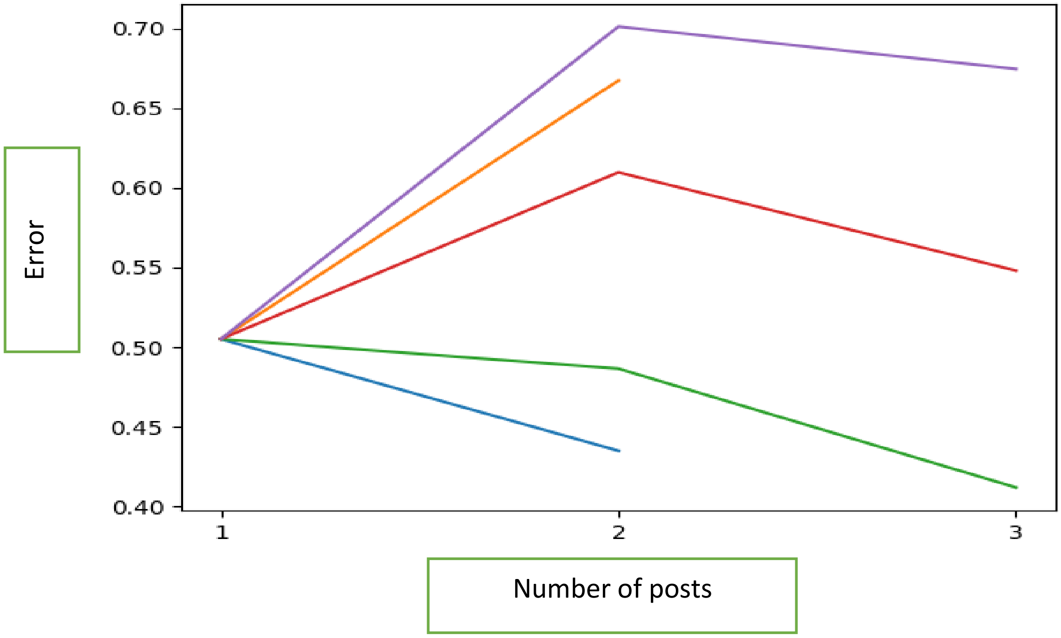


Figure 4.7 error value of trust for a fake source calculated using change in entity reaction (Ro) for a given initial trust value of 0.01

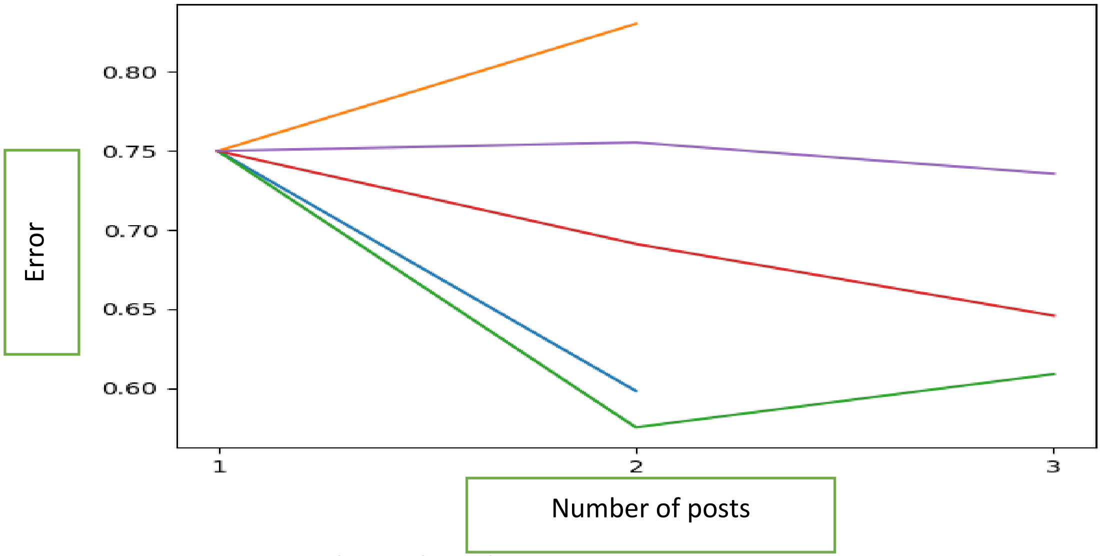


Figure 4.8 error value of trust for a fake source calculated using change in entity reaction (Ro) for a given initial trust value of 0.5

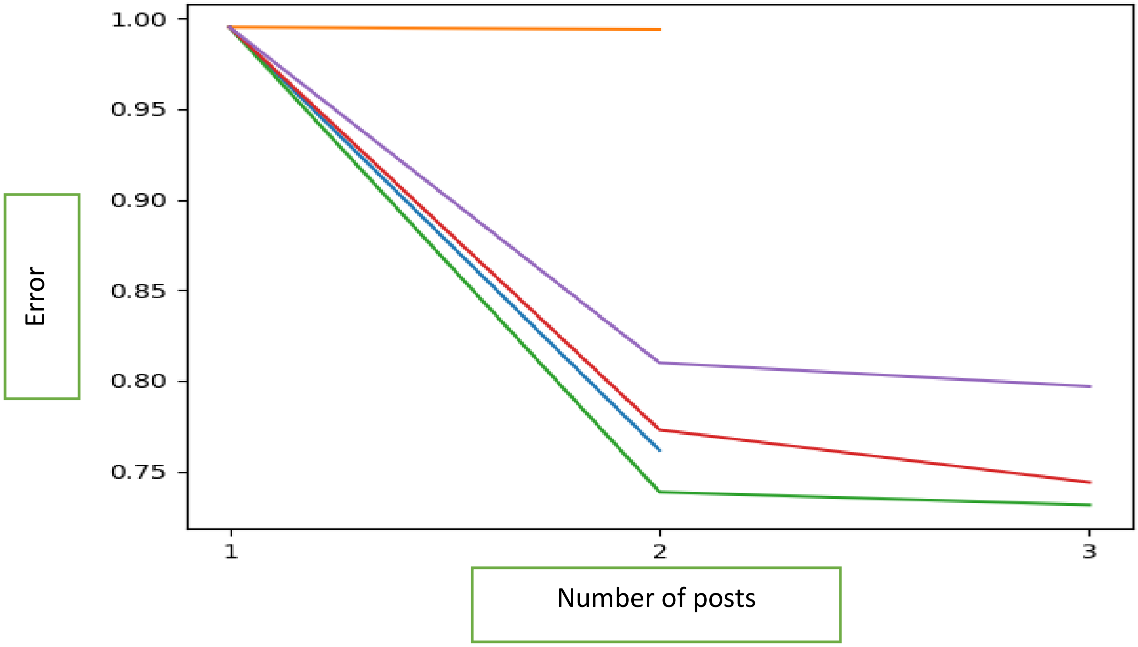


Figure 4.9 error value of trust for a fake source calculated using change in entity reaction (Ro) for a given initial trust value of 0.99

As we can see similar to the event reaction change, we can see that in Figure 4.7 where its initial value is given 0.01 or almost incorrect. It has low error value to those others that have closer to 1 initial value. In Figure 4.8 it has lower error value to that of Figure 4.9. The reason is that its closeness of its initial value to 0.

As shown from the figures, one source has a lower error than the other sources even those it has higher initial value. It has 0.61 value in Figure 4.8 where other 2 sources have 0.64 and 0.715 values in Figure 4.7 similarly its Figure 4.9 value is 0.73 whereas other 3 sources have 0.77,0.75 and 0.75. this is because of its reaction change to the entity is lower than those of the other sources.

As we can see to most of the sources the error value decreases as the posts increase. The change in reaction has an effect on increasing the trust value of the posts in the future posts. And all the sources start at one point this is because there is no change in a reaction at the beginning of the post. We can’t compare any reaction change of a source at post 1.

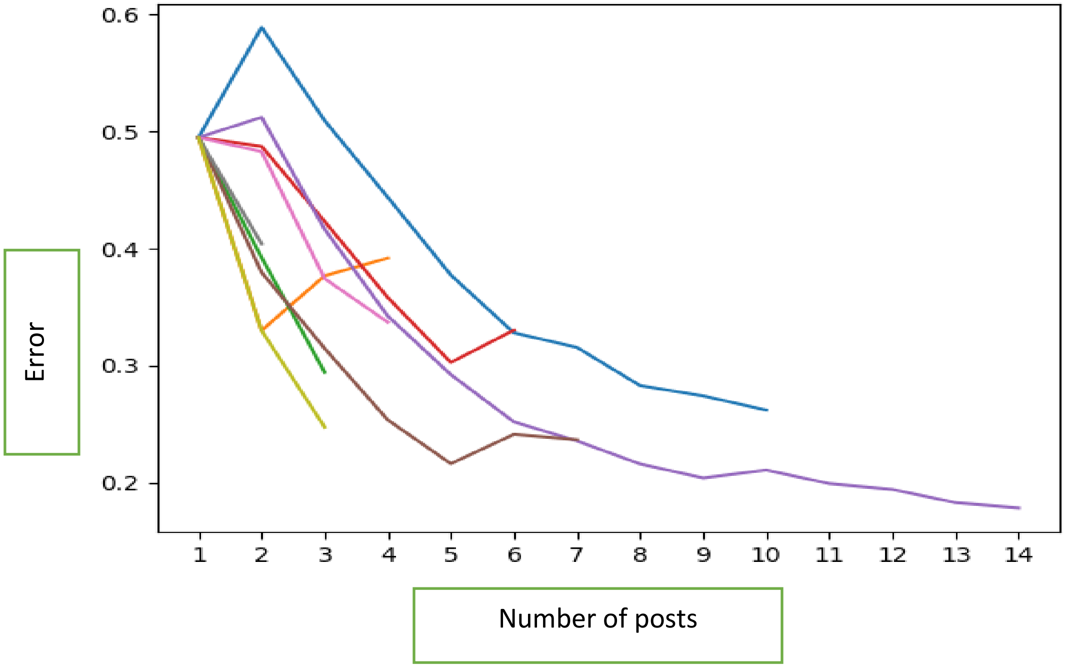


Figure 4.10 error value of trust for a genuine source calculated using change in entity reaction (Ro) for a given initial trust value of 0.01

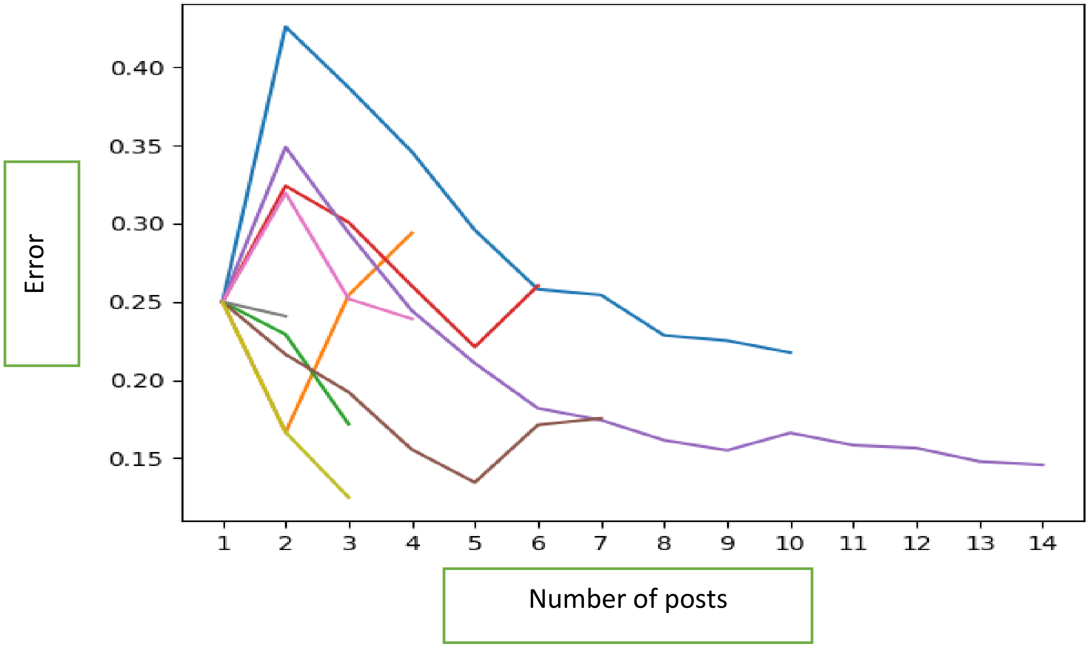


Figure 4.11 error value of trust for a genuine source calculated using change in entity reaction (Ro)for a given initial trust value of 0.5

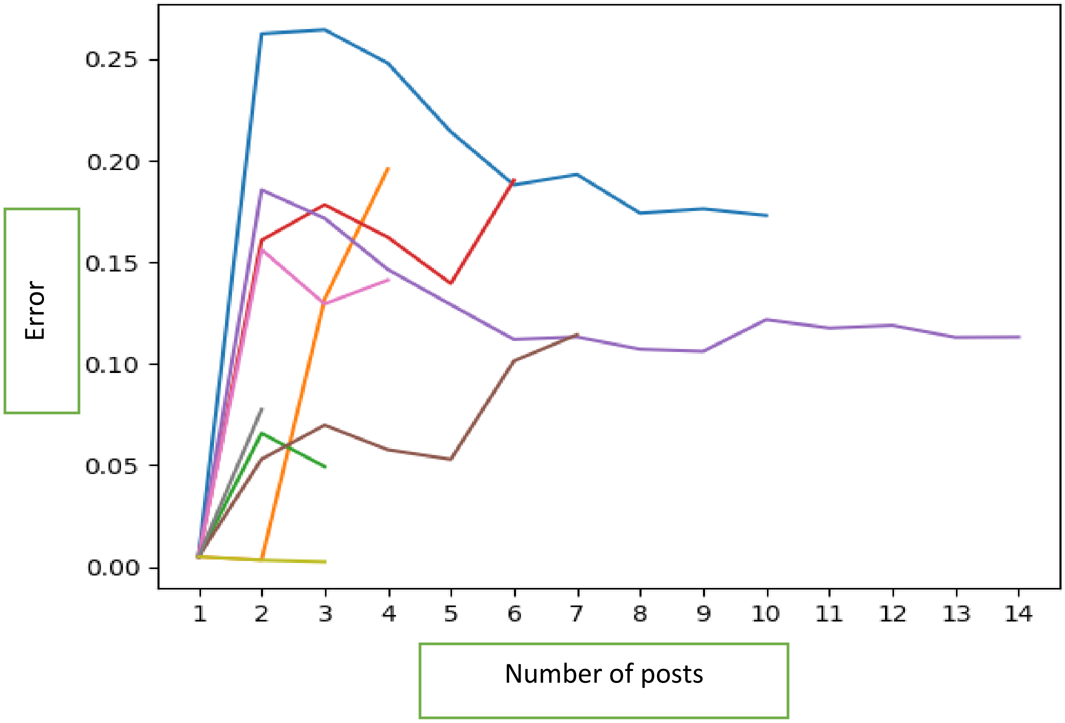


Figure 4.12 error value of trust for a genuine source calculated using change in entity reaction (Ro) for a given initial trust value of 0.99

From the above figures, we notice that, Figure 4.12 has lowest error value as compared to Figure 4.11 and Figure 4.10. This is because the sources are genuine, and in Figure 4.12 we are assuming that the sources have an initial value of 0.99 which is almost true or correct. Figure 4.11 has lower error value than Figure 4.10. It is because it has nearer initial value to the truth than Figure 4.10.

Similar to the fake sources, all the genuine sources start at a specific position because in post 1 the change in the reaction is 0 since, only their trust value is calculated. After post 1 we can calculate the change in the reaction of the source to the entity.

4.5. The bias of a source

The bias of source to a specific source is expressed by giving a different view to the entity from that you give to other entities or you have a different view than others. In here the bias of a source is the average of the change in reaction of a source to an event and change in reaction of a source to an entity. In the following Figures, we showed the effect of bias on a sources trust value.

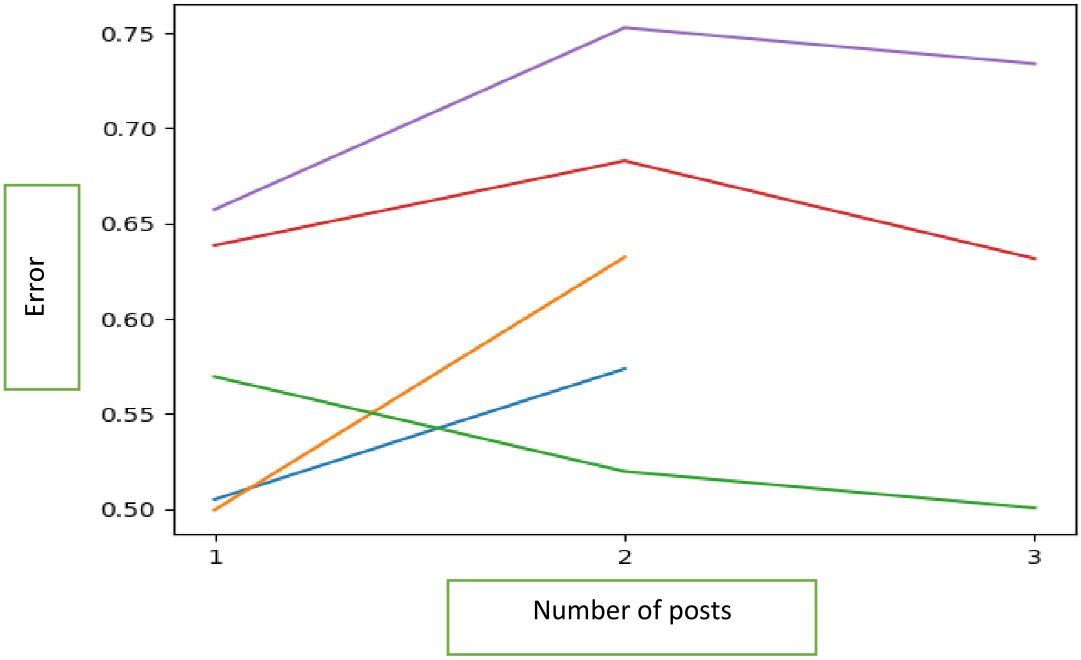


Figure 4.13 error value of trust for a fake source calculated using bias (B) of source for a given initial trust value of 0.01

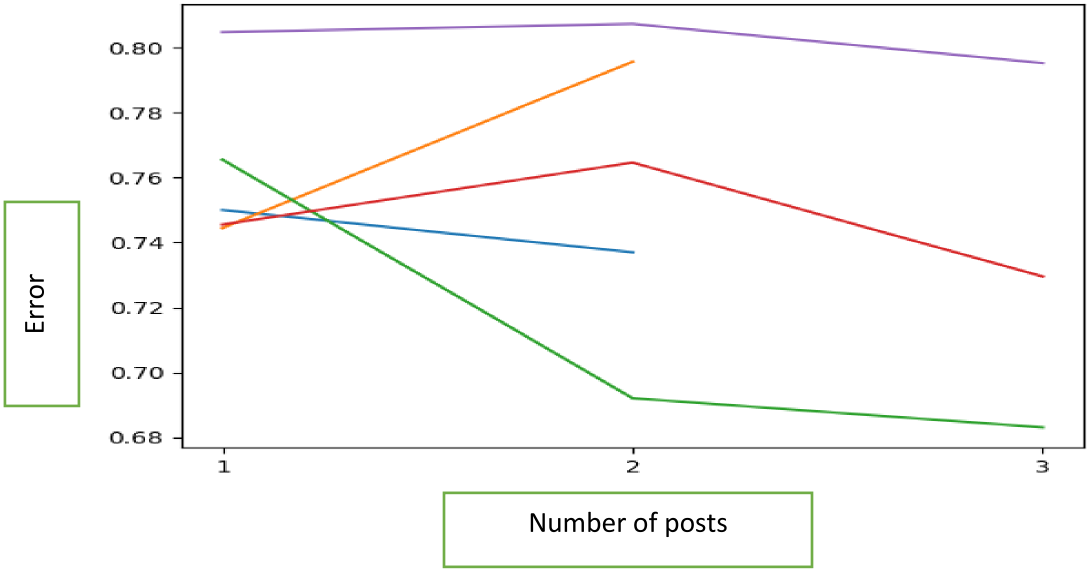


Figure 4.14 error value of trust for a fake source calculated using bias (B) of source for a given initial trust value of 0.5

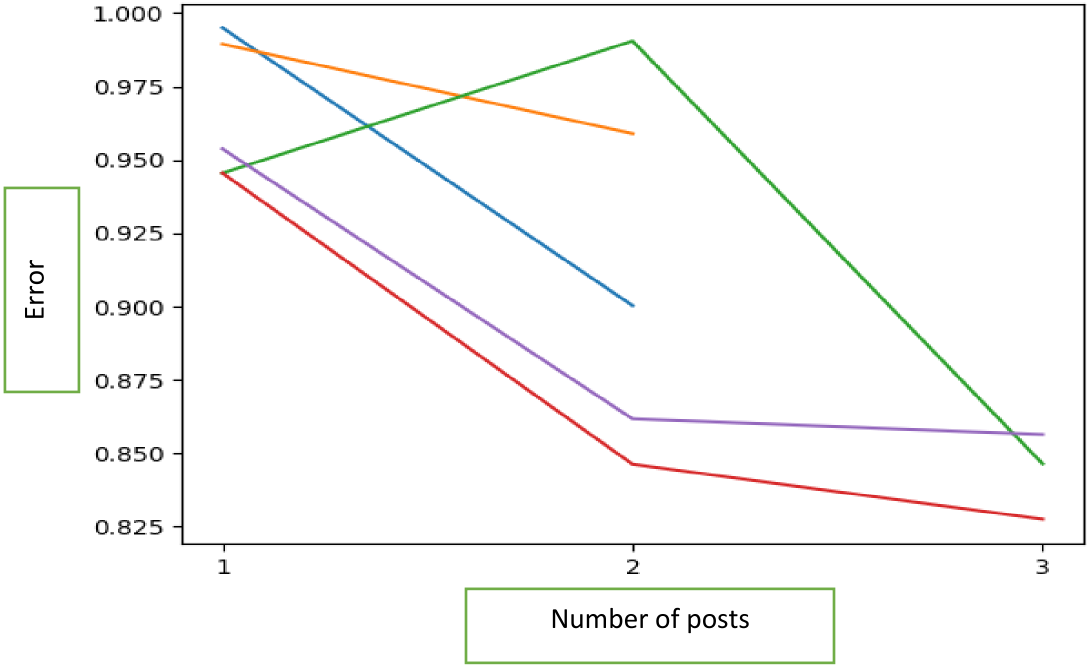


Figure 4.15 error value of trust for a fake source calculated using bias (B) of source for a given initial trust value of 0.99

As shown from the figures it has almost the average of both of the reactions error value. This is because it in cooperates both the change in the reaction of an event and an entity. In here also the initial value is affecting the error value of the sources. As the initial value is close and close to zero its error value decreases because the sources are a fake source.

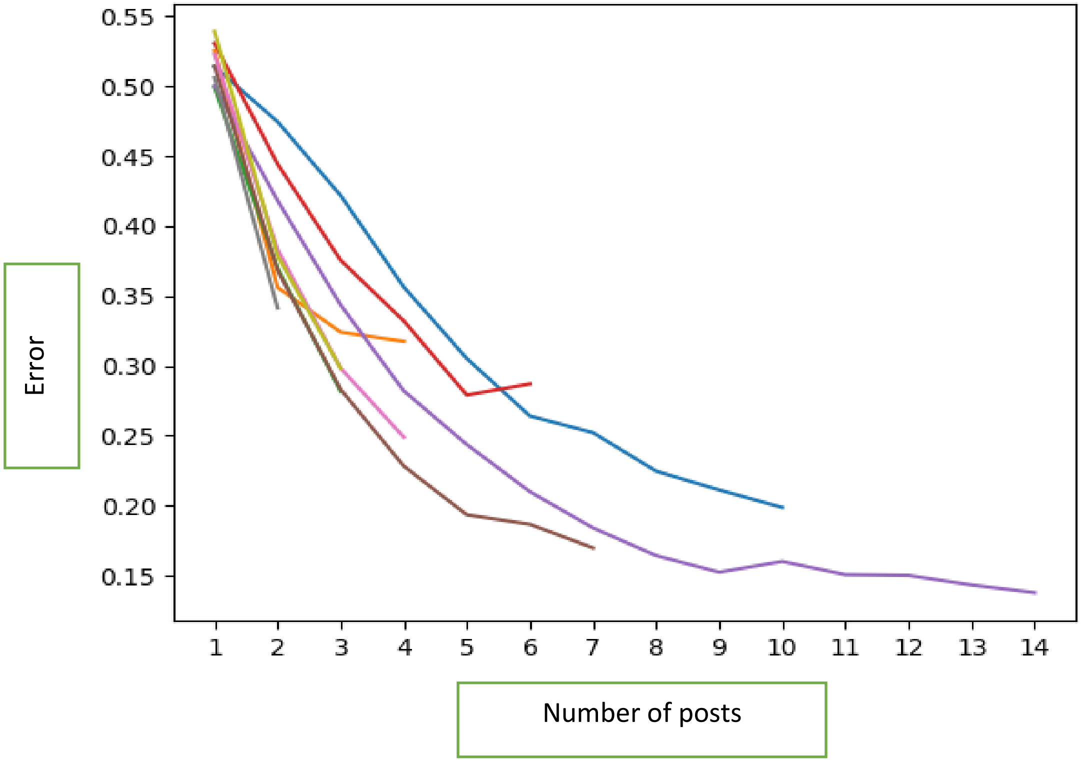


Figure 4.16 error value of trust for a genuine source calculated using bias (B) of source for a given initial trust value of 0.01

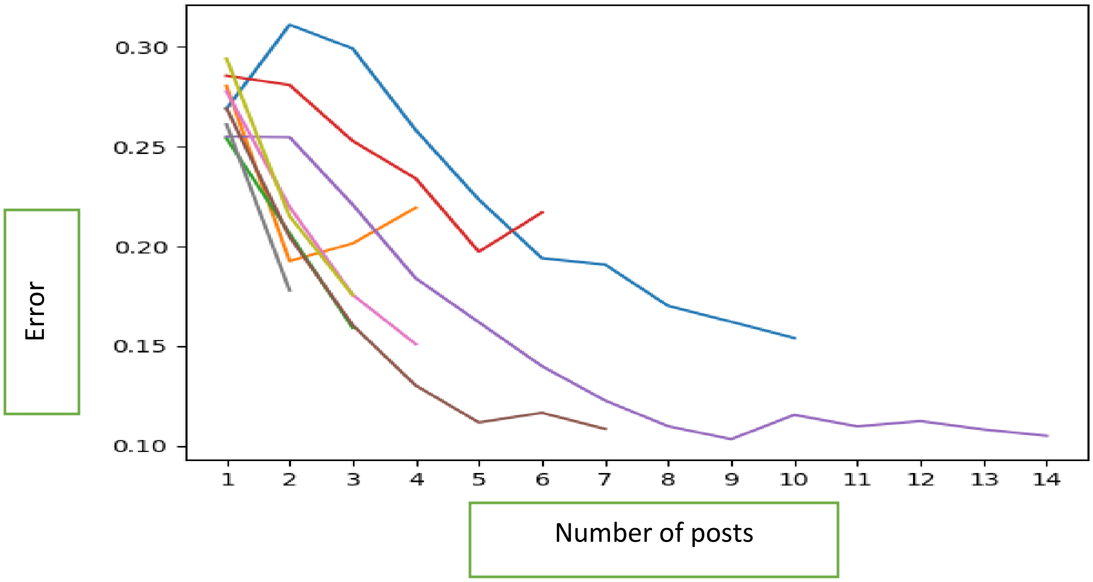


Figure 4.17 error value of trust for a genuine source calculated using bias (B) of source for a given initial trust value of 0.5

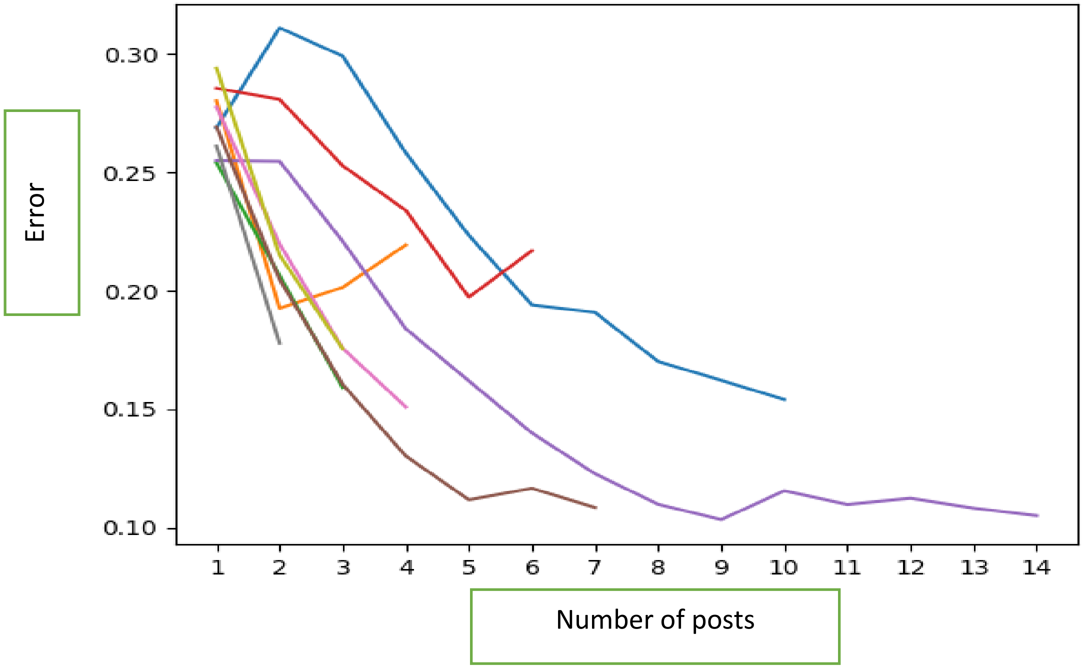


Figure 4.18 error value of trust for a genuine source calculated using bias (B) of source for a given initial trust value of 0.99

Similar to the fake source this also has almost an average error value of both the reactions at post one and two. But as we go deeper it has its own error value. Also, as the sources initial value get closer to 1 its error value decreases because its sources are genuine.

As we can see from both the genuine and fake source as the posts increase the error value decrease. This is because the trust value converges from an initial value to the real trust values of the sources. This will make their error value to decrease.

At the starting of the figures there is a higher difference in error value this is created with the given initial trust value. But as the posts go the error value difference gets smaller. This show as that the sources are converging to a point. If a source doesn't combine fake and genuine post at some post it will converge to one trust value.

As shown from the figure the trust values that are calculated using bias are in between the values of that are calculated using a reaction to an event and change in opinion about an entity. This is because it incorporates both the change in the reaction of an event and an entity. In here also the initial value is affecting the error value of the sources. As the initial value is close and close to zero its error value decreases because the sources are a fake source.

4.6. The overall accuracy of the system

For different initial trust value, we have calculated the accuracy of the system. In the table, we can see that the initial trust value and accuracy for fake posts and for genuine posts. The initial trust value is the way of telling the system that a source which hasn't written anything or is writing for the first time. If it is genuine (initial trust value 1), fake (initial trust value 0) or giving it initial trust value between genuine and fake (0-1). When we set the initial trust value, we are given them past trust value, this means we are telling the system if the source were genuine or fake in the past. So, if we tell the source was genuine and the source is writing a genuine post the system will have high accuracy and if we tell the source was fake and the source is writing fake news the system will have high accuracy. Whereas if we tell the system the source is genuine and the source is writing fake posts it will have low accuracy and if we tell the system the source is fake and the source is writing genuine posts it will have low accuracy.

Initial trust value	Accuracy for fake posts	Accuracy for genuine posts
0.01	0.6144	0.6486
0.1	0.5830	0.6752
0.2	0.5348	0.7047
0.3	0.5132	0.7343
0.4	0.4782	07638
0.5	0.4433	0.7934
0.6	0.408	0.8229
0.7	0.3735	0.8524
0.8	0.2385	0.8720
0.9	0.2236	0.8115
0.99	0.2014	0.7486

Table 4.2 accuracy of the system for different initial trust value

As shown from table 4.2 we can see the accuracy of genuine posts increase as it gets closer to 1 and fake posts increase its accuracy as it gets closer to 0. This is the effect of the initial trust value. As the initial value gets closer to 1, we are telling the system the source is tend to be genuine source than the fake source. As the initial value gets closer to 0, we are telling the system the source tends to be fake source than the genuine source. This have an effect on the result of the accuracy of the genuine and fake posts. Because the trust value analysis depends on the past trust value of the source (past history of the post).

CHAPTER FIVE
CONCLUSION AND RECOMMENDATION

5.1. Conclusion

This research shows how we can use the sentiment value of a source to a specific entity in evaluating the trust value of the source. We have created a method on how to calculate the trust value of the source based on sentiment analysis, knowledge base, and the voting system.

We have used the sources reaction to an event. This is evaluated in relation to another source's reaction to the event. A source's difference in reaction to an event have an effect on its trust value. If the source has a different reaction to an event from the average post by other sources. It will have a higher probability of affecting its trust value.

Another thing we used is the change in reaction to an entity. If a source has a sudden change in reaction to an entity it will have a higher effect on its trust value. So those two reactions are used with the knowledge base and voting system in a calculation of the trust value of the source.

It is essential to use the voting system and knowledge-base when calculating the trust value of a source. The voting system can be used as a mechanism for crosschecking. And the knowledge-base is used to predict the future trust value with the help of historic past trust values.

By using bias which is the average of both the reactions towards the event and an entity. We reduced it error in calculating the trust value of a source. Using bias in calculating the trust value of the source using the knowledge base and voting system we can have a higher accuracy on the trust value.
The main contribution of this study is to include sentiment analysis into the calculation of trust analysis. It studies the effect of sentiment in the calculation of the bias of the source. This study

tries to change the sensationalism of a journalist to mathematical bias that can be used in calculating the trust of the journalist.

The research has shown the effect of sentiment on trust value. This was the main issue of the research. Even though the research has accomplished its main objective. This research was done on posts that are related to Donald Trump. This has its own effect on the research. Because we are using one entity to calculate the trust value its accuracy is low. To make it higher, there should be more than one entity and the topics of the posts should be diverse. This will make the system universal for any kind of posts that are written on social media.

5.2. Recommendations

In order to decrease the error, we can add many attributes when calculation the trust value but this will have an effect on the performance of the method. When dealing with posts, there are millions of posts that are written every day. But as a recommendation we think those lists below can decrease the error with the effect of a little bit the performance.

- We recommend that this research should experiment on big data. This means with more than one entity and more than one subject type. By collecting large sums of claims from different sources on different entities and subject type (politics, sport, entertainment, science, religion, etc.). This will show as a very best method of using a sentiment from the three types we have used and can be used to implement the system in the real world.

- We have used the average of both reactions when calculating the bias of the source. This is not true in the real world. One can have more effect than the other. So, we recommend further to be studied in order to find which affect most and give a multiplier quotient to each reaction values.

- This method can be manipulated by adding well-known facts, general knowledge's and other topics which are not related in order to make the trust value higher. So, it is good to create a method that uses trust distribution between the facts of the post.

- We have calculated accuracy for 10 initial trust value. But in order to work for any kind of source, there should be an empirical study to find the percentage of sources telling the truth at the starting point.

- We recommend that research should be done on more than one entity and the relationship between the entities should be studied. The relationship between the entities and create a mechanism on how to make a source to an entity relationship based on other entity related to the entity.

REFERENCES

Anuta, D., Churchin, J., & Luo, J. (2017). Election Bias: Comparing Polls and Twitter in the 2016 U.S. Election.

Barretto, M. C., & Morajkar, S. (2017). Sentiment Analysis Tools and Techniques: A Comprehensive Survey.

Byungkyu Kang, J. O. (2015). Believe it or Not? Analyzing Information Credibility in Microblogs.

Collomb, A., Costea, C., Joyeux, D., Hasan, O., & Brunie, L. (2013). A Study and Comparison of Sentiment Analysis Methods for Reputation Evaluation.

D’Andrea, A., Ferri, F., Grifoni, P., & Guzzo, T. (2015). Approaches, Tools and Applications for Sentiment Analysis Implementation.

DataReportal. (2018). *Worldwide digital population*. Retrieved from https://www.statista.com: https://www.statista.com/statistics/617136/digital-population-worldwide/

Facebook. (2018). *Number of Facebook users worldwide*. Retrieved from https://www.statista.com: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Gilbert, C., & Hutto, E. (2015). VADER: A Parsimonious Rule-based Model forSentiment Analysis.

Hamido, F., & Jie, L. (1987-2017). Knowledge-Based Systems.

Hargrove, T., & H Stempel, G. (2007). Use of Blogs as a Source of News Presents Little Threat to Mainline News Media. *Newspaper Research journal*.

Jeff, P., & Dan, R. (2011). Making Better Informed Trust Decisions with Generalized Fact-Finding.

JENS, B., & FELIX, N. (2009). Data Fusion.

Jeong, S., Noh, G., Oh, H., & Kim, C. k. (2016). Follow spam detection based on cascaded social information.

Liu, S., Wang, Y., Zhang, J., Chen, C., & Xiang, Y. (2017). Addressing the class imbalance problem in Twitter spam detection using ensemble learning.

Miller, Z., Dickinson, B., Deitrick, W., Hu, W., & HaiWang, A. (2014). Twitter spammer detection using data stream clustering.

Mitra, Tanushree, & Gilbert, E. (2015). CREDBANK: A Large-Scale Social Media Corpus with Associated. *Ninth International AAAI Conference on Web and Social Media*.

Puranjay, S. (2015). *2 Million Blog Posts Are Written Every Day, Here's How You Can Stand Out*. Retrieved from http://www.marketingprofs.com/articles/2015/27698/2-million-blog-posts-are-written-every-day-heres-how-you-can-stand-out

Sandra, B., Rebecca, C., & Anna, G. (2017). *Fighting Fake News.* The Floyd Abrams Institute for Freedom of Expression.

Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). Fake News Detection on Social Media: A Data Mining Perspective.

Silverman, C., Shaban, H., Singer, J., & Strapagiel, L. (2016). Hyperpartisan Facebook Pages Are Publishing.

Soroush, V., Deb, R., & Sinan, A. (2018). THE SPREAD OF TRUE AND FALSE NEWS ONLINE.

Statista. (2017). *Level of trust in selected online news sources*. Retrieved from https://www.statista.com: https://www.statista.com/statistics/620130/online-news-sources-trustworthiness/

Statista. (2018). *Perceived frequency of online news websites reporting fake news stories in the United States*. Retrieved from https://www.statista.com: https://www.statista.com/statistics/649234/fake-news-exposure-usa/

Studyandexam. (2018, 9 18). *Subject, Predicate and Object*. Retrieved from studyandexam.com: http://www.studyandexam.com/subject-predicate.html

Thangavel, R. (2018, 9 18). *english for students.* Retrieved from Subject Object Predicate: http://www.english-for-students.com/Subject-Object-Predicate.html

Twitter. (2018). *Twitter: number of monthly active users*. Retrieved from https://www.statista.com: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/

Urken, A. B. (2011). Voting Theory, Data Fusion,and Explanations of Social Behavior.

Usman, A., AL-KHARUSI, M. I., & Awwalu, J. (2015). Application of Sentiment Analysis in Business Intelligence.

V.Mäntyl, M., Graziotin, D., & Kuutila, M. (2017). The evolution of sentiment analysis—A review of research topics, venues, and top cited papers.

Wang, & Yang, W. (2017). “Liar, Liar Pants on Fire”: A New Benchmark Dataset for Fake News Detection.

Xin Luna, D., & Felix, N. (2009). Data Fusion – Resolving Data Conflicts for Integration.

Xin Luna, D., Evgeniy, G., Heitz, G., Horn, W., Murphy, K., Sun, S., & Zhang, W. (2014). From data fusion to knowledge fusion.

Xin Luna, D., Evgeniy, G., Murphy, K., Dang, V., Horn, W., Lugaresi, C., . . . Zhang, W. (2015). Knowledge-Based Trust: Estimating the Trustworthiness of Web Sources.

Zhao, J., Lu, X., Wang, X., & Ma, Z. (2015). Web Information Credibility: From Web 1.0 to Web 2.0.

APPENDIX

Appendix 1 sample data

[{'source': 'static.politico.co', 'text': 'Sen. Mitch McConnell said a filed spending measure is the "result of many, many hours of bipartisan work across the aisle." Getty McConnell plays hardball in spending fight Mitch McConnell is playing hardball forcing Democrats into a take-it-or-leave-it position on a must-pass ', 'time': '20160824152021', 'value': '1'}]

Source: indicate the source of the post. The person or user that wrote the post.

Text: post that is posted on twitter part of the main post that is taken from the source website.

Time: is the time the post was posted in here the first 4 digit is the year next 2 digits are the month and the following 2 digits are day and the remaining 6 digits are the hour, minute and second.

Value: is the value of the post 1 mean genuine and 0 mean fake post.

Appendix 2 sentiment value

Sentiment value of the 233 posts which contain fake and genuine. Y-axis represents the type of data 1 for a genuine post and 0 for a fake post. Whereas x-axis represents sentiment value which varies from -1 to 1 were -1 means very negative and 1 means very positive. If it is 0 it means it is neutral. Figure 8 show sentiment value of 120 genuine posts and 113 fake posts. Figure 9 show 94 posts' sentiment value of the posts that contain the entity, Donald Trump.

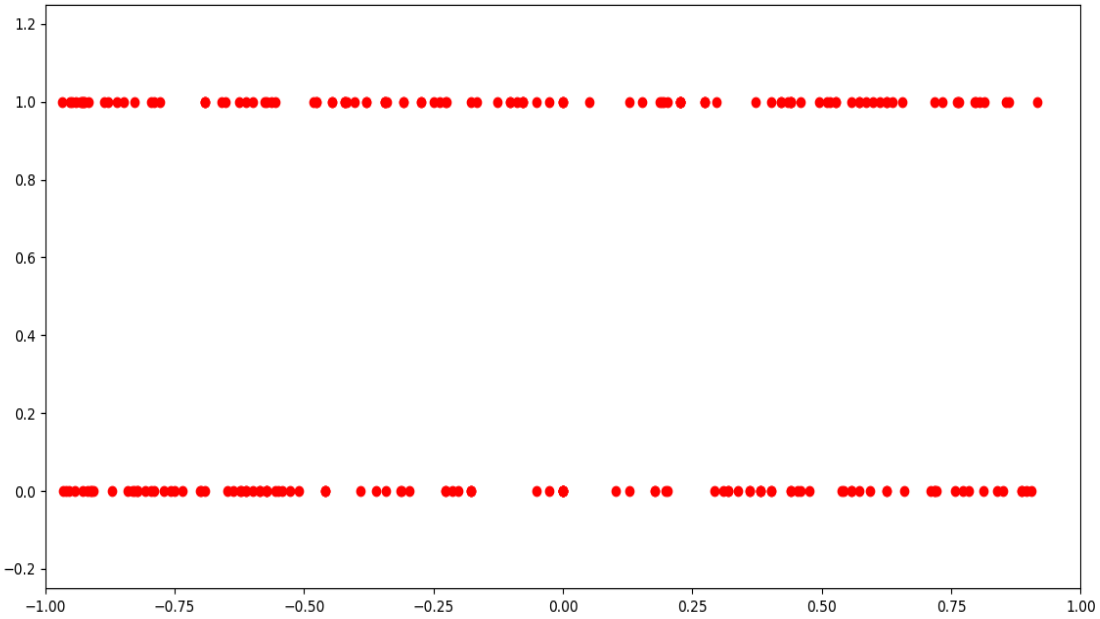


Figure 6.1 sentiment value for 120 genuine and 113 fake posts

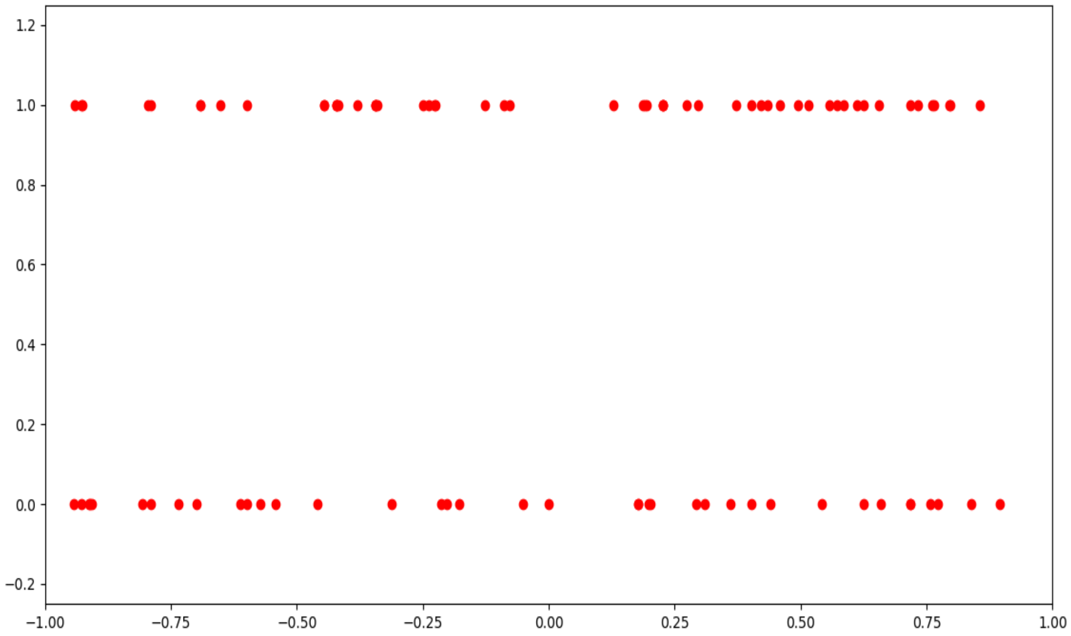


Figure 6.1 sentiment value of posts that contain the entity, Donald Trump