International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-10, August 2020

Identification of Fictitious Messages in Social Network using E-Hits and Newsapi

Jeeva. R, Muthukumaran. N

Abstract*: Social network has become a primary resource for users to send and receive the foremost up-to-date data and trend the present events. Currently, most of the social network contains the fictional content that was created by the influential spreaders wherever the message originality and therefore the spreader identity cannot be found which affects the end users. The proposed models to discover fictitious messages are verifying the contextual integrity with the trained classifier using large datasets. But the problem lies in updating of datasets with the recent or trending events from trusted sources in a regular interval. In the existing model, Hypertext-Induced Topic Search (HITS) method has been used for rating posts based on hub score and authority score. The hub score is calculated based on how many posts are posted or liked or tagged by the user and authority score is calculated based on how many users liked or tagged a post. If the user who ranks high in hub score tries to trend the low ranked post in authority score, the user will be marked as spreader. But the problem lies in the identification and verification of the posts that ranks in authority score. In our proposed system, we have enhanced the HITS algorithm by adding a third mechanism called top score which assigns weightage for every post based on the time they have posted. The time and content of the post has been verified by the integrated new model NewsAPI. Based on the three scores, the posts are filtered and matched with the news collected from NewsAPI. The news or posts that have not been matched either with the context or with the time will be marked as fictitious.

Keywords: Authority score, HITS, Hub score, NewsAPI, Spreader, Top score

I. INTRODUCTION

The wide accessibility of computerized information in social network and the colossal client pool offers an intriguing inquiry on evaluating the impact of clients dependent on the user cooperation after some time. This online connection over the social network offers ascend to an ongoing association arrange that speaks to a basic mechanism for spreading and catches significant qualities on how data can diffuse. A noticeable model is Facebook in which the computerized parts (e.g., user status, posts, photographs, recordings and connections) of a Facebook client are visible on a Facebook Timeline by other people who can communicate with them, (for example, tapping the Facebook Like support button for a post). These online communications are recorded on the Facebook Timeline that again prompted more cooperation.

Here, the spreading procedure expands the vulnerability of different clients to the equivalent; this outcomes in the progressive spread of a computerized message from a couple of clients to some more. It is fascinating to examine the spreading stimulus of an advanced verbal motor turning over from a chose not many. It is reasonable to expect that a particular Facebook user who has a digital message in the past that has garnered many other Facebook users' interaction (say using the Facebook Like endorsement button) is likely to attract similar level of interaction with future posting of similar digital messages. This is because this digital interaction (e.g., the Facebook "Like") captures the desire to share similar opinions or disposition, and typically comes from Facebook users who are already socially close or shows the willingness to interact. Also, it captures the connectivity relationship among users in the online social network. This is useful such as when this particular Facebook user wants to schedule a cascade of endorsement for a digital marketing message or is a business entity that maintains a Facebook presence and wants to spread the word of new commercial products. By examining the past record on Facebook Timeline, this particular Facebook user can determine other Facebook users who are deemed influential enough in a viral marketing strategy Online social networks (OSNs) have billions of clients and they have been a dynamic hotspot for different research disciplines. OSNs' lens furnishes analysts and researchers with excellent prospects to comprehend people at scale and to break down human standards of conduct, generally unthinkable. The data generated by OSNs users have been used in different applications. The huge rise of OSNs driven by communication technology revolution seriously remodeled the stage of human connections. Human communications facilitated by OSNs could defy the worldly and spatial impediments of conventional correspondences in a remarkable way, in this manner displaying subjectively new layers of social interactions, which concurs and works together with current connection layers to rethink the multiplex informal organizations. These several network layers or communication channels in a multiplex network don't act totally independently or conditionally.

Revised Manuscript Received on August 30, 2020.
***** Correspondence Author
Jeeva. R*, Department of Computer Science & Engineering, Thamirabharani Engineering College, Tirunelveli, India. E-mail: jeeva3710@gmail.com
Muthukumaran. N, Department of Electronics and Communication Engineering, FX Engineering College, Tirunelveli, India. E-mail: kumaranece@gmail.com

Similarly, identifying influential spreaders in an OSN by demonstrating a single layer interaction network and disregarding the other interaction will create an incomplete relationship data portrayal, and therefore, unverifiable distinguishing proof outcomes. Therefore, various sorts of interaction between users ought to be considered for better understanding the information diffusion process and precise influential spreaders identification.

II. RELATED WORK

One of the most popular tools in twitter is the list of trending topics that capture the hottest emerging trends and topics of discussion. Using this feature, people can quickly gather news about a particular topic or learn at glances which are the topics on which most people speak. But the increasing microblogging concept [1] paves the way for spammers to disperse malicious tweets. In this paper, spam messages have been identified using feature extraction based on statistical text analysis. This method calculates the probability distribution of texts in three language models and determines the degree of divergence between them. The divergence value classifies tweets into reliable and suspects. The suspicious tweets are those that link to a web page used for task classification and the reliable tweets become part of the thread of tweets language model used for evaluating the system. Online Social Networks (OSNs) [3] have been a origin of privacy to deal with and its problems. These privacy concerns have even increased along the past decade due to many real privacy incidents being echoed in the media and users being more aware of potential privacy issues. The exchange of inappropriate information and the undesired dissemination of previously exchanged information has become one of the privacy threats in OSN. In this paper, a computational model of implicit Contextual Integrity for OSNs has been used which includes an information model and an agent model i.e Information Assistant Agents (IAAs). IAAs are capable of learning contexts and their associated information sharing norms albeit these are implicit or unknown a priori. Each IAA monitors the knowledge exchanges of its user and supported this it infers: (i) the various contexts during which information sharing is to happen; (ii) the relationships among the individuals in each context; and (iii) the knowledge sharing norms of every context. If IAAs detect a potential violation of the information sharing norms like sharing a event or a message outside the user relationship circle, it alert the users, who have the last word on whether sharing the knowledge or not. Microblogging websites has become popular platforms for information dissemination and sharing. Massive fake microblogging accounts, which are known as social spammers, post masses of spam messages for various purposes, including conducting social advertising, collecting user's personal information, promoting affiliate websites and so on. a unified approach has been proposed to detect social spammers and spam messages via categorizing the social contexts into the user-content relationship, user–user relationship and content–content relationship of micro-blogging users and messages. An efficient optimization algorithm based on ADMM [4] marks the messages as spam when many users post it with the same hash tag or refer the same URL. The spam rate value has computed for each social context category to mark the spam as positive or negative.

Aleksei Romanov, Alexander Semenov, OleksiyMazhelis and JariVeijalainen identifies fake identities play a critical role in advanced unresolvable threats and are also involved in other malicious activities. This research concentrates on the literature study of the state-of-the-art research aimed at detecting fake profiles in social network. The methods to identify fake social media accounts can be classified into the categories targeted on reviewing individual user accounts, and the methods to capture the coordinated activities spanning a large group of user accounts. This work portrays the role of fake identities in advanced unresolvable threats and covers the mentioned approaches of detecting fake accounts in social network [6]. Ermelinda Oro, Clara Pizzuti, Nicola Procopio and Massimo Ruffolo proposed a method which had a capable to find fake users who controls over the user network, and participating in sharing posts about the familiar topic. The activity of the user depends upon exploring the contents of the posts shared by them, to express their comments on it, by structuring them in a three-layer network. Each layer represents users, posts and reserved words, along with its interactions among the users of it. The connections between the layers are classified as triplelets (u, p, r) denotes the content that a user u comments on an post p with the reserved word r. [7].An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.Author (s) can send paper in the given email address of the journal. There are two email address. It is compulsory to send paper in both email address.

III. HITS

In existing system, an influential spreaders has been identified based on both topic and post information in the social network. System contains the information about users and automatically detects the correct number of topics and identifies event related posts to higher precision by using a Hypertext- Induced Topic Search (HITS) based Topic-Decision method (TD-HITS). Every post has its authority score that shows its importance in it. Eventually, each user has their hub score that shows the participation in the network. The primary function of the iterative model is the mutual relationship between the post importance and a user's participation. For instance, a user who has posted or shared many high-significance posts is more likely to make greater impact than other posts in expressing a real-life event. Mutually, a post that is shared by many high participated users is more likely to be a high significance post. A user's participation can be calculated by summation of the authority scores (i.e., quality) of all posts posted or responded upon by that user, and the significance of a post can be represented by the sum of the hub scores (or quality) of all the users who have shared that post. From its conclusion, a user with maximum authority score is an influential user and post with maximum hub score is a high quality post.

But the problem lies in the verification of the post content. To verify, the system relies on the high user participation in the network. The chances of false positives are high like fake news can spread higher than the real if more number of users has shared or any other activity has performed.

IV. ENHANCED HITS

The user in the social network can do many activities like posting, like post tag a post etc. For every action of the user, his/her profile will be assessed to determine the activity in the network that results in hub score. Each post in the social network will be assessed individually assessed how much activity has been carried out in it. Based on the both scores, the top trending posts has been identified and weightage has been assigned form new to old. Then the posts have been verified with NewsAPI to determine the post originality level.

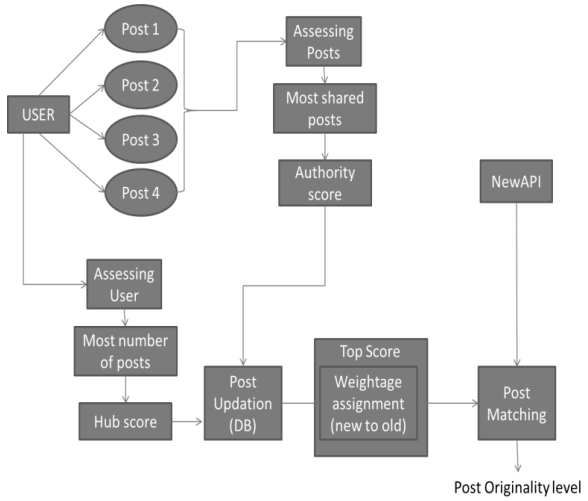

Fig. 1.Framework of E-HITS

A. User authentication and posting

The user has to register first and signs in using his/her unique username and password. The user has to be authenticated by verifying his/her records with database and allow to login into the newsfeed page. In newsfeed page, the user can able to view the posts, share them and also post content in newsfeed in text form. Each user has to be identified with unique user id. The user has to be post his/her content in the text area field in the newsfeed. Null content posts are not able to be posted. Each post has to be assigned with unique post id. All the posts posted by the user are saved in a database with the post posted time, unique post id and the content of the post. Each post share by the user has to be stored in database with the unique post id and the concern user id who share it.

B. Score Calculation

All posts are taken into account for calculating the hub and authority scores. The posts are retrieved from database and the scores are calculated and stored in the base. The following scores have to be calculated by using our enhanced HITS algorithm. They are a) Hub Score: It calculates the activity of user with multiple posts. Hub score calculation is based on the single user who posts multiple posts in the system. The total count of the user interaction with posts are said to be the hub score of that user. Similarly, the hub score can be calculated for every user. b) Authority Score: It calculate the activity of post by the users. Authority score calculation is based on number of share for a single post by users in the system. The total count of the post interaction with users are said to be the authority score of that post. Similarly, the authority score can be calculated for every post. c) Top Score: It calculates the activity of post within specified time limit. It is also similar as authority score whereas it calculates the score based on the single post that can share by multiple post within the particular time limit. The post which was shared within one hour of posting, then it have an weightage of 1 and sharing of post greater than one hour and less than five hours have 0.75 also have a value of 0.5 and 0.25 for hours greater than five and less than ten and hours greater than ten and twenty four respectively. Top score can be calculated by the sum of all the values of each time limit. The value of the each time limit can be calculated by the product of the weightage and the total number of shares within the particular time limit. The top score is calculated for the posts which are posted within the twenty four hours from the current time.

C. News Collection

The news has to be collected from the various news site by using the NewsAPI key when the button was clicked and also the action performed by the user. Then the obtaining news has to be categorized by using the json parser and only the headlines of the news have to be considered. The delimiters present in the news are removed. The news headlines are collected and stored in the database along with its corresponding date and its source of origin.

D. Post filtering and classification

The post filtering process has been achieved by two levels. a) Filtering post based on time Constraint. b) Filtering post based on Top Score. a) Filtering post based on time Constraint. The time limit will set to filter the post among the vast quantity of posts. The time difference can be calculated for each post by considering the post creation time and the current time. If the time difference satisfies the time constraint that posts are consider for the next level of filtering. b) Filtering post based on Top Score. The posts filtered in first level have to be considered for calculating the top score. The top score value have be calculated based on sharing post in time constraint criteria given by the admin and they are sorted based on top score value in highest to lowest. Among them the top high quality posts are considered for verification with news. The posts and their corresponding post created date are considered. Based on that date value the news has to be filtered from database. The posts are matching with news and give a matching result in terms of percentage. The percentage level above 60 % shows that the post is most likely to be true. Such posted are classified and marked as a verified post in the newsfeed.

E. E-HITS Algorithm

Input:
No of posts (d), No. of users (n)
Post time (ptime)

```
Output:
Post originality level (POL)
While (Active)
begin
   if(post activity)
   begin
      d.a=d.a+1
   end
   n-DB_CHECK(post)
   if(n exists)
   begin
      n.h=n.h+1
   end
   if(ptime<60 mins)
   begin
      d.t=1
   else if(ptime>60 mins and ptime<300 mins)
      d.t=0.75
   else if(ptime>300 mins and ptime<1440 mins)
      d.t=0.5 to 0.25
   else
      d.t=0
   end
   POL=NewsAPI(Max(d.a and d.t)
end
```

V. EXPERIMENTAL RESULTS

A simulated experiment has been conducted over 500 interactions that include 3 users with 3 posts with various timings (10 samples). Three users are represented as u1, u2 and u3. p1, p2 and p3 are represented as posts. Based on the interactions, number of times the post has been shared and number of posts that a user has shared was collected are shown in Table I.

Table- I: User activity count and Post shared count

S.No	No of shares			No of Activity in posts		
	u1	u2	u3	p1	p2	p3
1	182	161	154	172	156	169
2	172	160	165	172	163	162
3	162	177	158	154	158	185
4	171	162	164	166	179	152
5	165	156	176	151	170	176
6	183	147	167	161	162	174
7	179	169	149	162	154	181
8	158	177	162	161	173	163
9	176	165	156	155	166	176
10	174	155	168	155	173	169

$$\text{Hub score} = \frac{\text{No of activity in posts}}{\text{Total no of interactions}}$$

$$\text{Authority score} = \frac{\text{No of activity of the user}}{\text{Total no of interactions}}$$

Table- II: Hub score and Authority score for the 500 interactions

Hub score			Authority score		
p1	p2	p3	u1	u2	u3
34.61	31.39	34.00	36.62	32.39	30.99
34.61	32.80	32.60	34.61	32.19	33.20
30.99	31.79	37.22	32.60	35.61	31.79
33.40	36.02	30.58	34.41	32.60	33.00
30.38	34.21	35.41	33.20	31.39	35.41
32.39	32.60	35.01	36.82	29.58	33.60
32.60	30.99	36.42	36.02	34.00	29.98
32.39	34.81	32.80	31.79	35.61	32.60
31.19	33.40	35.41	35.41	33.20	31.39
31.19	34.81	34.00	35.01	31.19	33.80
31.59	34.21	34.21	36.02	30.78	33.20

Table II shows the values of hub scores and authority scres of the users and the interacted posts. The post time for each interaction has been noted and a weightage has been assigned that starts to decrease if the activity has been done on the same post and the post has been evaluated with NewsAPI that returns the similarity score are shown in Table III.

Table- III: Post weightage and API Similarity

Post weightage			API Similarity		
p1	p2	p3	p1	p2	p3
1	1	1	0.45	0.56	0.7
0.75	1	1	0.45	0.56	0.7
0.75	0.75	1	0.45	0.56	0.7
0.75	0.75	0.75	0.45	0.56	0.7
0.25	0.75	0.75	0.45	0.56	0.7
0.25	0.25	0.75	0.45	0.56	0.7
0.25	0.25	0.25	0.45	0.56	0.7
0.125	0.25	0.25	0.45	0.56	0.7
0.125	0.125	0.25	0.45	0.56	0.7
0.125	0.125	0.125	0.45	0.56	0.7
0.0625	0.125	0.125	0.45	0.56	0.7

The Top score has been calculated as

Top score=Hub score*Post weightage*API Similarity

The value will be varied even for the same user for the same post as the computation takes the post time as primary value.

Table- IV:Top score for 500 interactions over 10 samples

Top Score		
p1	p2	p3
15.57	17.58	23.8
11.68	18.37	22.82
10.46	13.35	26.06
11.27	15.13	16.06
3.42	14.37	18.59
3.64	4.56	18.38
3.67	4.34	6.37
1.82	4.87	5.74
1.75	2.34	6.2
1.75	2.44	2.98
0.89	2.39	2.99

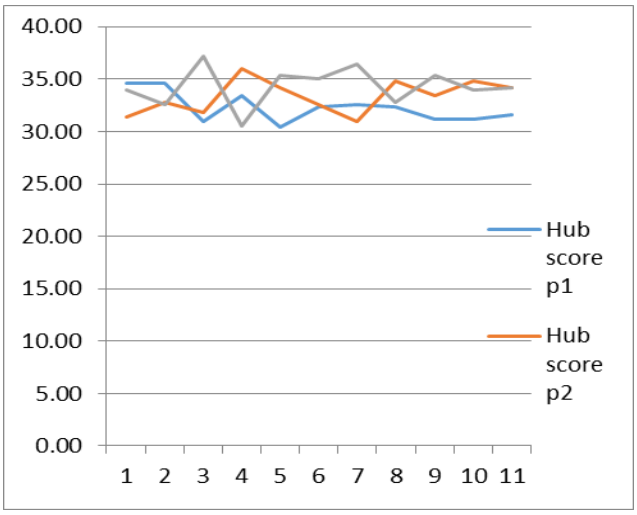

Fig. 2. Hub score mapping for 3 posts over 500 interactions

In Fig. 2, post p3 has high trust value over 35 compared to p2 and p1. The level has been maintained for the 10 samples that may look like a genuine post. In Fig. 3, the post p3 has only over 4% originality when it reaches the 10th sample. This deduces the post that has been repeatedly shared in order to increase the score to make it real.

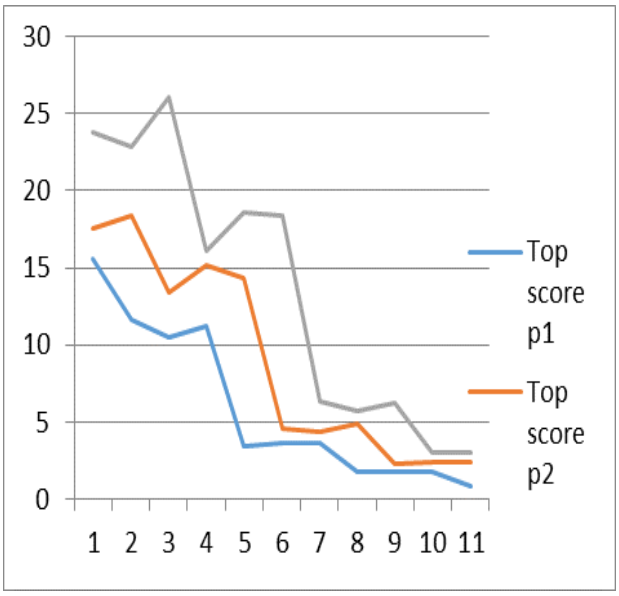

Fig. 3. Top score mapping for 3 posts over 500 interactions

VI. CONCLUSION

This proposed approach filtered the high quality post based on the time constraint. It largely reduces the occurrence of the fictitious message that is shared by the influential users in online social network. Moreover this approach verifies the trustworthiness of the post by verifying it with the news which is gathered from the trusted news site NewsAPI. At last, a post which has a matching result above 60% with news shows that the post is most likely true.

REFERENCES

1. Juan Martinez, Lourdes Araujo "Detecting malicious tweets in trending topics using a statistical analysis of language", Vol. 40, No. 8, 2013.
2. Daniel Moise, Anca Francisca Cruceru "An empirical study of promoting different kinds of events through various social media networks websites", Procedia - Social and Behavioral Sciences 109, 2014.
3. Natalia Criado, Jose M. Such "Implicit Contextual Integrity in Online Social Networks", 2015
4. Xiaoming Fu, Jar-Der Luo, Margarete Boos, "Social Network Analysis: Interdisciplinary Approaches and Case Studies", 2016.
5. Aleksei Romanov, Alexander Semenov, Oleksiy Mazhelis and Jari Veijalainen "Detection of Fake Profiles in Social Media", 13th International Conference on Web Information Systems and Technologies, 2017.
6. Ermelinda Oro, Clara Pizzuti, Nicola Procopio, Massimo Ruffolo, "Detecting Topic Authoritative Social Network Users: a Multilayer Network Approach", IEEE Transactions On Multinetwork, Vol. 20, Issue 5, May 2018.
7. A. Aldhaheri and J. Lee, "Event Detection on large social media using temporal analysis", in Proc.7thAnnu. computing and communication workshop and conf., Las Vegas, NV, USA, pp.1-6, 2017.
8. Leilei shi, yan wu, lu liu, xiang sun, and liang jiang, "Event Detection and Identification of Influential Spreaders in Social Network Data Streams," Big Data Mining And Analytics, pp.34–46, vol 1, no.1, 2018.
9. Meet Rajdev, "Fake and Spam Messages: Detecting Misinformation during Natural Disasters on Social Network", All Graduate Theses and Dissertations - 4462, 2015.
10. Sandeep Sirsat, Dr. Vinay Chavan, "Pattern Matching for Extraction of Core Contents from News Web Pages", in 2016 Second International Conference on Web Research (ICWR).
11. Stuart E. Middleton, Symeon Papadopoulos and Yiannis Kompatsiaris, "Social Computing for Verifying Social Network Content in Breaking News", IEEE Internet Computing, DOI 10.1109/MIC.2018.112102235, 2018.
12. Wenhao Zhu, Song Dai, Yang Song and Zhiguo Lu, "Extracting News Content with Visual Unit of Web Pages", IEEE Communication Surveys & Tutorials, Vol. 16, No. 4, 2014.
13. Zhen Tan, Chunhui He, Yang Fang, Bin Ge and Weidong Xiao1, " Title-based Extraction Of News Contents For Text Mining", IEEE Access, Volume 6, October 2018.

AUTHORS PROFILE

Jeeva R received B.E degree in Computer Science and Engineering from Scad College of Engineering & Technology, Tamilnadu, India in 2011 and M.E degree in Computer Science and Engineering from Joe Suresh Engineering College, Tamilnadu, India in 2013. He is currently pursuing PhD at the Department of Information and Communication Engineering, Anna University, Chennai, India. He is working as a Assistant professor in Department of Computer Science and Engineering at Thamirabharani Engineering College, Tamilnadu, India.

Dr. N. Muthukumaran was born in Kaniyakumari, Tamilnadu, India, in 1984. He received the B.E Degree in Electronics and Communication Engineering, M.E Degree in Applied Electronics and the Ph.D Degree in Information and Communication Engineering from Anna University, Chennai, India in 2007, 2010 and 2015 respectively. He is currently working as a Professor& Research centre lab, Department of Electronics and Communication Engineering in Francis Xavier Engineering College, Affiliated to Anna University Chennai, Tirunelveli, Tamilnadu, India. His major research interests are in the field of Digital Image/ Signal Processing, Multimedia Image/ Video Processing/ Compression, Digital and Analog Very Large Scale Integration circuit design. Since 2006 he has published more than 42 International Journals like Springer, IEEE, Elsevier and 64 National/International conferences papers. He has published 11 International Books which is related to Engineering Students. He has actively participate and organized more than 102 research related events like National and International Workshop, Faculty Development Program, Seminar, Symposium, Conference and Short Term Courses Delivered & Attended. Currently, he is serving as Editorial and Reviewer Board Member of 24 International Anna University Chennai Recognized Annexure I, Annexure II Journals. He has collaborated and life time member of more than 19 various Memberships body Association like IEEE, ISI, WCECS, UACEE etc.