iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3197

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Toward Detecting Malicious Activities in Online Social Network through User Behavior

S. Nabila[1], S. Banupriya[2], S. Kiruba[3], M. Karpagaselvi[4]
[1, 2, 3, 4]*Final year, Department of Computer Science and Engineering*

Abstract: ***Social networks consist of context-sensitive and relational data while also including a considerable amount of malicious content.***
It has turned out to be troublesome to clarify the genuine semantic estimation of distributed substance for the identification of client practices.
Without comprehension the logical foundation, an integrated social media content analysis platform that leverages three levels of features, i.e., user-generated content, social graph connections, and user profile activities, to analyze and detect anomalous behaviors that deviate significantly from the norm in large-scale social networks.
Several types of analyses have been conducted for a better understanding of the different user behaviors in the detection of highly adaptive malicious users. In the proposed method, propose a directed graphs, to detect fraudulent users in OSNs.
In this, given a training dataset we estimate the posterior probability distribution for each user and uses it to predict a user's label.

I. INTRODUCTION

Online social networks social (OSNs) have become indispensable platforms for interacting with people, processing information, and diffusing social influence. However, a large number of users on OSNs are fraudulent , e.g., spammers, fake users, and compromised normal users.

Adversaries use these fraudulent users to perform various malicious activities such as disrupting democratic election and influencing financial market via spreading rumors distributing malware as well as harvesting private user data. Therefore, detecting fraudulent users is an urgent research problem.

Indeed, this research problem has attracted increasing attention from multiple communities including data mining cyber security, and networking.

Depending on the used information sources, we classify existing approaches into two categories, global structure based methods and local features based methods[1][2]. Several types of analyses have been conducted for a better understanding of the different user behaviors. A list of key contributions can be described as follows.

A. A complete entity-awareness user behavior analysis model is proposed herein that upholds the widespread cognizance of entities represented by users to achieve accuracy in the judgment process of malicious activity detection. The model has four layers: a social sensing layer, a data acquisition and preparation layer, a data storage management layer, and an analysis representation layer. All layers work together, similar to a complete algorithm, to analyze the user behaviors and feed the results into a proposed classification model that manipulate five machine-learning algorithms to assess user profiles and detect malicious users.

B. An essential methodology is used for the harvesting of characteristics pertaining to YouTube and Twitter users, for example their contacts, original posts, and reactions. These characteristics are applied to perfect an algorithm for Sybil detection.

C. The core idea of this study is the leveraging of interactions among OSN users, and more specifically, contextual activity information related to such users, which can be a valuable source of insight that cannot be deduced by simply looking at the macro picture or applying a new malicious activity detection technique.

D. The effectiveness of our system is measured through a comparison of different user profiles from two types of social network, Twitter and YouTube. The observations applied in our system are users or activities, and the positive class is normal. In this scenario, a classifier with high specificity is preferred rather than the recall rate because users classified as normal might propagate harmful content, causing a threat to security. Therefore, the first preference is given to alleviate the false positives (FPs).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

II. RELATED WORKS

A. *Using Global Graph Structure*

These methods [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14] often leverage a set of labeled fraudulent nodes and/or labeled normal nodes. Then they propagate these label information among the graph to predict labels of the remaining nodes. The key insight of these methods is that a node is fraudulent (or normal) if it links to other fraudulent (or normal) nodes. We call these methods in order to stress their application to detecting fraudulent users.

1) *Using Directed Social Graphs:* Fraudulent users detection in social networks can be modeled as binary classification on directed graphs. For instance, Twitter's follower-followee network is a directed graph, and detecting fraudulent users can be viewed as a binary classification problem for nodes in the directed graph. To the best of our knowledge, guilt-by-association methods [12], [13], [14] on directed graphs are all based on random walks. Specifically, Distrust Rank [13] and CIA [14] assign an initial score for each node based on a set of labeled normal nodes. Then, they use random walks to propagate the reputation scores to the remaining nodes. They also restart the random walks from the initial reputation scores with a certain probability called restart probality These methods can only leverage labeled normal nodes [12] or labeled fraudulent nodes [13], [14], but not both, which limits their detection accuracies.
2) *Using Undirected Social Graphs:* Some guilt-by-association methods [3], [4], [5], [6], [7], [8], [9], [10], [11] assume symmetric relationships between nodes. They often assume the graph satisfies the homophily property, i.e., two linked nodes tend to share the same label. In principle, one can apply these methods to detect fraudulent nodes in directed social graphs via transforming them into undirected graphs. However, a directed graph has richer structural information than its undirected version [15]. Transforming a directed graph into an undirected one oversimplifies the graph structure and achieves limited accuracy. there are two ways to transform a directed graph to an undirected one. One way is to keep an undirected edge between two nodes once they are connected by directed edge(s). This way is not adversarially robust. In particular, fraudulent nodes can easily inject a large amount of edges with normal nodes in the undirected graph. For instance, on Twitter, a fraudulent user can follow many normal users, all of which will be kept in the undirected graph. As a result, fraudulent nodes well embed in the normal nodes and the undirected graph does not satisfy the homophily property, limiting the detecting accuracy of those guilt-by-association methods. The other way is to keep an undirected edge between two nodes if they are connected via bidirectional edges. However, such transformation cannot leverage unidirectional edges, which are useful for determining reputations of nodes.

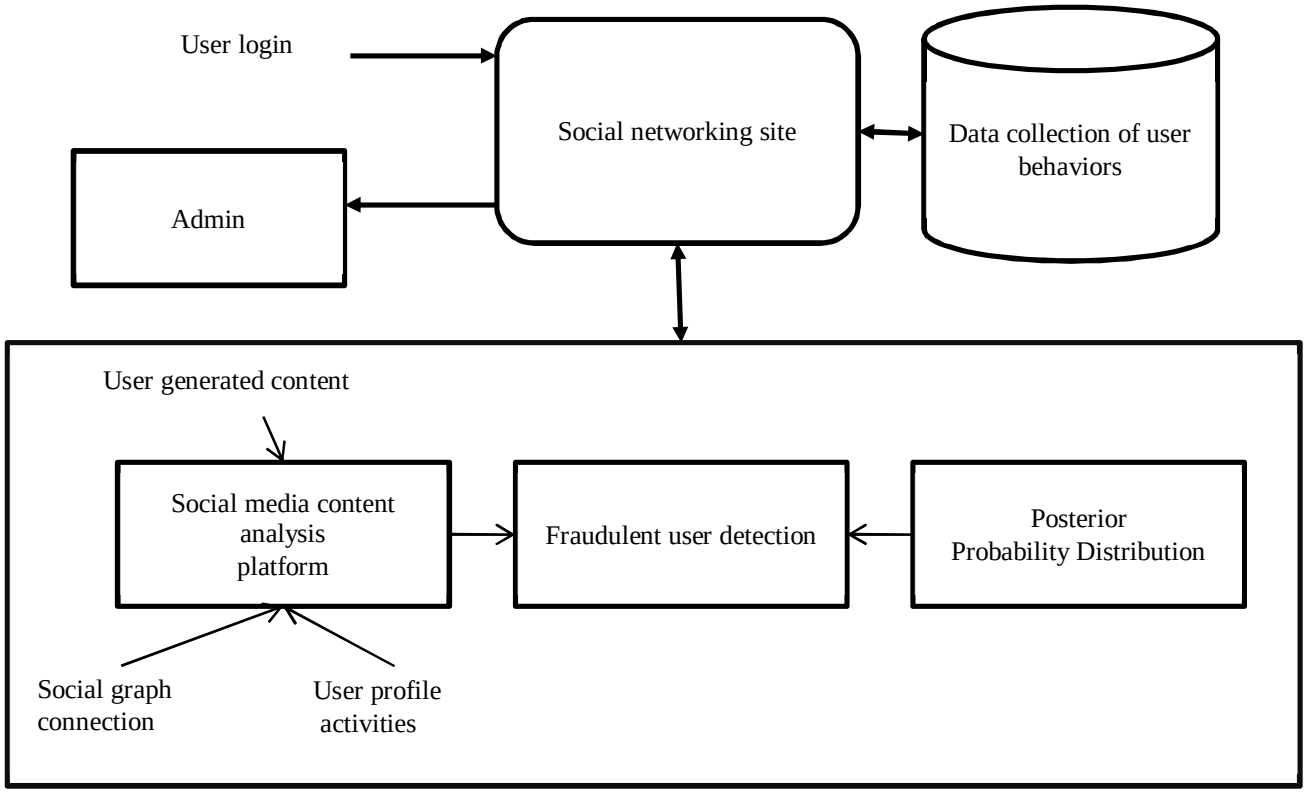
B. *Using Local Features*

Local feature based methods leverage a user's local subgraph Structure (e.g., dense subgraphs, a node's hop-2 neighborhood,and a node's ego-network) [16], side information (e.g., IP address, behaviors, and content) [18], [19], and possibly combine them with features from the global social structure [20], [21]. They rely on that fraudulent nodes have abnormal subgraph structures, behavioral analysis, linguistic analysis, and/or sentiment analysis. A key limitation of these methods is that they are not adversarially robust. Specifically, fraudulent nodes can evade detection of subgraph based methods via creating many fake nodes (e.g., an adversary can create many fake accounts on Twitter [1]) and manipulating links between them to change their subgraph structures as desired. Fraudulent nodes can also modify their side information to mimic normal nodes to evade side information based methods. Indeed, we found such fraudulent nodes in Sina Weibo, and our method can detect them. Producing a suspiciousness score can rank users, which serves as a priority list to aid human workers to find more fraudulent users within the same period of time. Our method produces a suspiciousness score for every user (i.e., the probability that a user is fraudulent).

III. OUR WORKS

In this work, we propose report based method on directed graphs, to detect fraudulent users in OSNs. we associate a binary random variable with each user to model its label, and then we design a novel pairwise Markov Random Field (pMRF) to model he joint probability distribution of all these random variables based on the directed social graph. Our pMRF incorporates unique characteristics of the fraudulent-user-detection and blocked them. (eg: we call an edge (u,v) unidirectional if the edge (v,u) in the reverse direction does not exist, otherwise we call the edge bidirectional. If two users are linked by bidirectional edges and have the same label, then our pMRF produces a larger joint probability. However, suppose u and v are linked by a unidirectional edge (u,v), on this means that u follows v, but v does not follow back to u. If u is fraudulent or v is normal, then whether the unidirectional edge (u,v) exists or not does not influence the joint probability under our pMRF, otherwise the edge (u,v) makes the joint probability larger.

IV. DETAILED DESIGN



Malicious Account Detection

A. *Social Networking Site*

The user register online social network site and login to the site through the registered user name. The admin monitor the registered user list and post.

B. *Data Collection Of User Behaviour*

This layer is closely coordinated with the previous one, teaming up to properly utilize the information originally collected from the selected social media and stored in the Hadoop file system. Hence, the raw data are transformed into well-defined trends that have informational value and that can be fed into the analysis representation layer. When the importation of external data is completed, it is possible to perform predefined operations aimed on cleaning the data sample, and the user has an active role in this process through the user interface.

C. *Malicious Account Detection*

1) Guilt-by association: We introduce a basic version of our GANG. Specifically, we first introduce intuitions on which report based. Second, we design a novel customized pairwise Markov Random Field (pMRF) to capture the intuitions. Third, we discuss how we leverage the pMRF to detect fraudulent nodes.

a) *Bidirectional Neighbors:* If a neighbor *v* is a bidirectional neighbor of *u*, then *u* tends to have the same label with *v*, e.g., both u and v tend to be fraudulent. This property is known as homophile. OSNs with fraudulent and normal nodes have the mophily property because normal nodes will not link to fraudulent nodes with bidirectional edges in most cases.

b) *Unidirectional Incoming Neighbors:* If *v* is an unidirectional incoming neighbor, then *v* is not informative for *u*'s label if *v* is fraudulent. This is because a fraudulent node can link to many other nodes (fraudulent or normal) in OSNs. For instance, in OSN, the follower followed network is a directed graph in which an edge(v,u) means that *v* follows *u*, and a fraudulent node could follow many other fraudulent or normal users. Therefore, being linked by a fraudulent node does not mean the node is fraudulent nor normal. However, when *v* is normal, *u* also tends to be normal.

2) Social media content analysis platform

a) *User Generated Content:* Community building and relationship building should be an important part of your social media marketing efforts. In this we focus on a shared images and videos.

b) *Social Graph Connection:* The success of OSN comes down the concept of the social graph connection. Photos, events and pages are connected with other information such as your relationship to your friend, stuff that you share, and photos that you tag.

c) *User Profile Activities:* We need to follow to create a successful social media profile that are your display name, your user name and url, your profile picture, your link, bio data are needed.

V. PERFORMANCE ANALYSIS

We introduce a basic version of our LBP. Specifically, we first introduce intuitions on which report based. Second, we design a novel customized pairwise Markov Random Field (pMRF) to capture the intuitions. Third, we discuss how we leverage the pMRF to detect fraudulent nodes.

A. Detecting Fraudulent Nodes

We leverage the above pMRF to detect fraudulent nodes. Suppose we are given a set of labeled fraudulent nodes denoted as *Lf* and a set of labeled normal nodes denoted as *Ln*. We set the parameter *qu* in node potentials as follows:

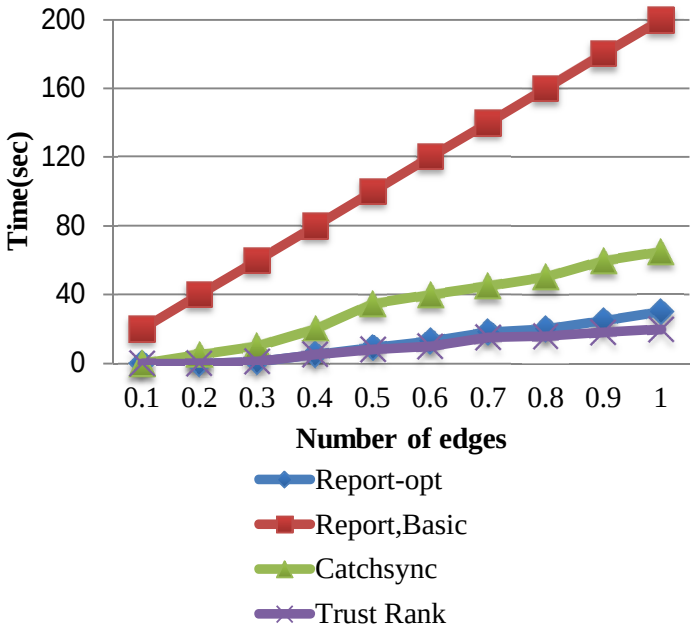
$$qu = \begin{cases} 0.5+\theta & \text{if } u \in Lf \\ 0.5-\theta & \text{if } u \in Ln \\ 0.5 & \text{otherwise} \end{cases}$$

where $0<\theta \leq 0.5$. Then, we compute the posterior probability distribution of a node *u*, i.e., $Pr(xu) = \Sigma xV/u\ Pr(xV)$. For simplicity, we denote by *pu* the posterior probability that *u* is a fraudulent node, i.e., $pu = Pr(xu = 1)$. We predict *u* to be fraudulent if $pu > 0.5$, otherwise we predict *u* to be normal.

B. Computing Posterior Probability Distribution

we use[22] to estimate the posterior probability distribution Pr(xu). LBP iteratively passes messages between neighboring nodes in the graph. This encodes that each node forwards a product over incoming messages of the last iteration and adapts this message to the respective receiver based on the homophily strength with the receiver. It stops when the changes of messages become negligible in two consecutive iterations or it reaches the predefined maximum number of iterations T. After this halts, we estimate the posterior belief Pr(xu) as follows:

$$Pr(t)(xu) \propto \varphi uv(xu, xv)\ \Pi k \in \Gamma(u) m(t) ku(xu),$$

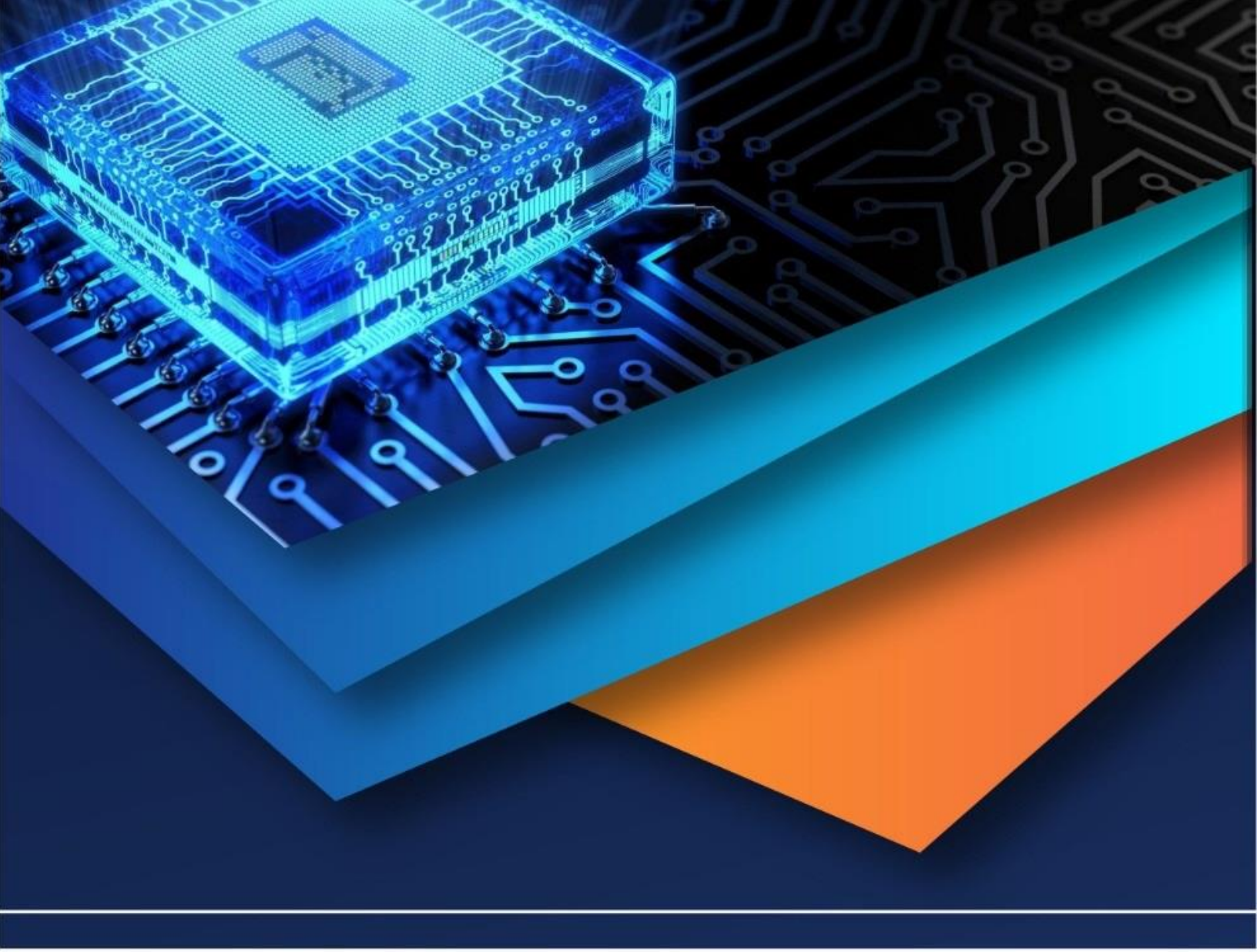


VI. CONCLUSION

In this work, we propose a report based method on directed graphs, to detect fraudulent users in OSNs. Based on the unique characteristics of the fraudulent-user detection problem in directed graphs, we design a novel pairwise Markov Random Field to model the joint probability distribution of the states of all users. In the basic version of report based method, we posterior probability distribution to perform inference. Furthermore, we optimize this to make it convergent and more scalable via eliminating message maintenance and approximating this by a concise matrix form. We compare report based method with various existing methods using a large-scale online social network with labeled fraudulent users and normal users.

REFERENCES

[1] N. Z. Gong, M. Frank, and P. Mittal, "SybilBelief: A semi-supervised learning approach for structure-based sybil detection," IEEE TIFS, vol. 9, no. 6, 2014.
[2] P. Gao, N. Z. Gong, S. Kulkarni, K. Thomas, and P. Mittal, "Sybilframe: A defense-in-depth framework for structure-based sybil detection," CoRR, 2015.
[3] N. Z. Gong, M. Frank, and P. Mittal, "SybilBelief: A semi-supervised learning approach for structure-based sybil detection," IEEE TIFS, vol. 9, no. 6, 2014.
[4] P. Gao, N. Z. Gong, S. Kulkarni, K. Thomas, and P. Mittal, "Sybilframe: A defense-in-depth framework for structure-based sybil detection," CoRR, 2015.
[5] B. Wang, L. Zhang, and N. Z. Gong, "SybilSCAR: Sybil detection in online social networks via local rule based propagation," in IEEE INFOCOM, 2017.
[6] J. Jia, B. Wang, and N. Z. Gong, "Random walk based fake account detection in online social networks," in IEEE DSN, 2017.
[7] H. Fu, X. Xie, Y. Rui, N. Z. Gong, G. Sun, and E. Chen, "Robust spammer detection in microblogs: Leveraging user carefulness," ACM Transaction on Intelligent Systems and Technology(TIST), 2017.
[8] S. Pandit, D. H. Chau, S. Wang, and C. Faloutsos, "Netprobe: a fast and scalable system for fraud detection in online auction networks," in WWW , 2007.
[9] G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil nodes using social networks," in NDSS, 2009.
[10] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in NSDI, 2012.
[11] S. Rayana and L. Akoglu, "Collective opinion spam detection: Bridging review networks and metadata," in KDD, 2015.
[12] Z. Gy¨ongyi, H. Garcia-Molina, and J. Pedersen, "Combating web spam with trustrank," in VLDB, 2004.
[13] B. Wu, V. Goel, and B. D. Davison, "Propagating trust and distrust to demote web spam."MTW , vol. 190, 2006.
[14] C. Yang, R. Harkreader, J. Zhang, S. Shin, and G. Gu, "Analyzing spammer's social networks for fun and profit," in WWW, 2012.
[15] N. Z. Gong and W. Xu, "Reciprocal versus parasocial relationships in online social networks," social Network Analysis and mining, vol. 4, no. 1, pp. 1–14, 2014
[16] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai, "Uncovering social network Sybils in the wild," in IMC, 2011



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY