International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Product Recommendation based on Sybil and Trusted Votes in Social Networks

Manasa S M, Tanuja R, Manjula S H, Venugopal K R

Social Networks is a platform which is easily accessible by normal users worldwide. Online Social Networks facilitates users online to get registered with ease of speed and create their own accounts to communicate with the social world for information gathering. This platform allows everyone to get registered online irrespective of their social behaviour. Users here are creating duplicate accounts that is creating Sybil in the network. By this Sybil online Social Networks are suffering for different kinds of Sybil attacks online. In social networks user's feedback and preferences play an important role in suggesting friends online or recommending products online. When collecting the feedback or preferences of any product online both Sybil user's and real user's data is considered as we are not differentiating the Sybil user or real user. From this products, recommended online will not have an efficient rating which would divert the buyers online. To over this problem we propose Sybil Community Detection Algorithm (SCD) and TrustRank Algorithm that bifurcates real user votes and Sybil users votes to fetch the efficient products online thus build secure online environment.

Keywords: Product Recommendation, Real user, Social Networks, Sybil, Votes.

I. INTRODUCTION

In today's speedy world people are connecting to each other through Online Social Networks (OSN), where one can express thoughts, likes, dislikes, share photos, share their interests, post day to day activities, and even recommend friends to others. OSNs are so popular that many of the vendor's market their products and services through online social networks. By tagging and advertising their products [1] and services enterprises expand their business and improve them by considering the reviews of consumers.

Sybil attacks are the major drawbacks in online social networks. Sybil attack is a mechanism of creating multiple copies of single identity. Sybil attacks ruin the reputation of the system by influencing it through user pseudonyms. Some interactive systems are cost effective which allow users to create their identities at a lesser cost. These kind of systems are more vulnerable to Sybil attacks. Sybils search for vulnerable systems and influence the system in a larger extent. Social networking systems accepts input from all users irrespective of their chain of trust associated with the trusted entity [2]. They consider each user identity as an individual user. Hence Sybil affects the entire system in a larger extent. i.e., creating multiple fake identities that introduces fake product, fake reviews, spams and malware. These Sybils target online social networking communities to get benefited. It is observed that the Sybils online forward spams and malware to various OSNs like Facebook, Twitter etc., Existing defence mechanism focus on using social graph structure to isolate fakes. In prior Sybil defences used the positive trust relationships among users, and rely on the key assumption that Sybils can befriend only few real accounts. Unfortunately, it is found that the people in real OSNs still have a non-zero probability to accept friend requests of strangers that is people do accept the friend request from others who are not known to the users [3]. Sybils will also get connected to the real users by sending a large amount of requests.

Here further explores the negative distrust relationships (e.g., in the form of rejected friend requests) among users, as Sybils have more distrust relationships [4] than trust ones with real users. However, this feature cannot be directly applied because attackers could hide their identities and promote them as trust user and get undetected or by generating many fake trust relationships among Sybils which intern affect the product voting and recommendation of those products to the true trusted users. To reduce this kind of fake relationships created by sybils helping to rise the voting of the fake products a concept of friend invitation interaction is considered [5]. This concept states that the interactions among users as a signed, directed network, with an edge directed from the sender to the receiver and a sign (1 or -1) indicates whether a friend request is accepted or the request is rejected. This graph is referred to as the friend invitation graph. Which depicts the number of request sent form normal user group and Sybil community group to each other and the number of request accepted by them.

VoteTrust here presents a system that leverages the friend invitation graph to detect Sybils, and their fake recommendation or the response to the product [6].

Manuscript published on November 30, 2019.
* Correspondence Author
Manasa S M*, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. Email: smmanasa609@gmail.com
Manjula S H, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. Email: shmanjula@gmail.com
Tanuja R, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. Email: tanujar.uvce@gmail.com
Venugopal K R, Bangalore University, Bangalore, India. Email:venugopalkr@gmail.com

The entire response on the product would bifurcate with real or trust, fake or Sybil, or normal users which will prevent from the votes collusion as well. This conclusion is obtained or the bifurcation is done by two line of defence mechanism. In the first line of defence takes place during the registration of the user. When user gets registered on to an application he/she is identified as trusted or Sybil by his/her authentication code [7]. Second line of defence mechanism initially the user is set as a unknown user, further depending on the user friend request is accepted or rejected he/she is considered as a trust, Sybil or normal user. When both line of defence mechanism is positive for a user then the product voted by him/her is considered as trusted vote. If both line of defence mechanism or either one of the defence mechanism is negative, then that users vote for the product is considered as Sybil vote. This detects Sybils present in each community which intern helps the growth of trusted user by identifying the Sybil users, in a controlled way [8].

A. Motivation

Social network is a service that help users to utilize specific information or resources online and get benefited. These services or information to be provided will be gathered from different sources and pooled up in a particular blog. These resource providers may be a malicious service providers or malicious users on social networking sites. When these resources are ready to use they should be reliable, because those resources would compromise on the privacy of the user. Hence a trust worthy mechanism is required to make sure that these collected resources are reliable and they don't compromise on privacy of the users.

B. Contribution

This work distinguishes a user as real user or Sybil user by its first line of defence. During the registration of the user status is set as unknown later second line of defence is friend invitation mechanism. For every user status is set as trusted, normal and Sybil based on the feedback received by the user interactions made on social networks. Distinguishing the votes of the user for the product, which help in fetching the efficient and guaranteed product online. Users rank (i.e., trust rank) are given based on the interaction scores. Individual Sybil community detection and Sybil community detection is also provided through user interaction feedback.

C. Organisation

The rest of the paper is organised as follows. Section II discusses the related work. Section III is the problem statement. Section IV describes system overview of the Product Recommendation on Social Networks based on Sybil and Trusted Users. Section V describes Vote Based Sybil detection. Section VI explains Community Status Detection. TrustRank of the user is discussed in section VII. Result analysis is done in section VIII. Paper conclusion is in section IX.

II. RELATED WORK

Social graph based approach, reputation system (symmetric, asymmetric approach), unsigned graph approach, feature based approaches and many more approaches are proposed for Sybil detection. Haifeng et.al., [9] used social graph based approach which is the unsigned graph approach to determine the Sybils in social networks. Leveraging the existing trust relationships between the users by human establishment which is bound to both the number and size of the Sybil group. Nodes are considered as a user, and if any directed edge exist between those nodes, it may be equated as a link between those users. It states that those two users are friends. It is based on the assumption that Sybils would be friend with only few real users.

Similarly, Vishvanath et.al., [10] used social graph based approach for Sybil detection. According to the research it stated that most of the algorithms developed by researchers for this schemes would differ in various means, but none of the algorithms detect Sybils. These schemes work very well in defining the connecting structure between the Sybil nodes and non-Sybil nodes. Here the concept of detecting Sybil in a community through algorithm is attempted, which try to finds the cluster of Sybil notes in the community. This research helped in providing the deeper understanding the Sybil defence schemes work in different social network analysing various algorithms. Wei et.al., [11] presented a Sybil defence mechanism using the social graph based schemes providing the Sybil defender algorithm which used various network topologies in social network to defend the Sybil attacks. Within the social graphs it performed limited number of random walks. This provided great efficiency in detecting the Sybil in a scalable to large online social networks. This effectively identifies the Sybil nodes and detects the Sybil community around the Sybil nodes.

Whereas Cheng et.al., [12] detect Sybil nodes by reputation mechanisms using the symmetric approaches, which uses the Eigen Trust provides that are more susceptible to Sybil attacks. Sepandar et.al., [13] used this reputation system. Eigen Trust to decrease number in authentic files on the network. In a peer-to-peer file sharing network, a unique trust value is assigned to each peer's in the network which help in decrease the number of downloads inauthentic files. It describes a secure and distributed methods based on the power iterations to compute the global trust value. As online social networks are very famous for communication and interaction and prove their effect on the users interaction. Jiang et.al., [14] provided a concept on understanding the latest Interactions in OSNs. The study led in the direction of interaction between the users various means were latest interactions, which are the passive actions. Study provided with the better and deeper understanding of the visible on latest user interactions in OSNs, this used the famous OSN of china Renren for the research of the latest interaction considering the characterizing the property with other OSNs and building the graph of the visitor's log that captured the browsing activity between online social network?

Gao et.al., [15] provided method to defect Sybils in the feature based approach. Where the Sybil are created for profitable malicious activity which includes click fraud, identify fraud, spanning malware distribution and many more.

Here an initial study to quantify and characterize spam campaigns which is been forwarded using the accounts that are created on the Online Social Networks. This provides a first type of study which measures and analyse attempts to spread malicious, contents on OSNs. Firstly, it analyse the message and identify the number of attempts made to spread this from various techniques. During the analysis the web address or the URL detected in the form of text subgraphs are built to represent potential social spam campaigns. It identifies the compromised accounts in the large OSNs. However, it cannot determine how these posts are soliciting the user to visit the malicious post and spread the malware.

III. PROBLEM STATEMENT

Xue et.al., [1] recommend a scalable defence mechanism to extend user level activities and detects Sybils with the help of friend invitation graph. Friend invitation graphs here detects the Sybil users and their collisions in communities on social networks but can't prevent their voting mechanism online. The proposed system ensures that the Sybil votes and real user votes are bifurcated. Once these votes are bifurcated each product online will have the rating with two parameters i.e., real user votes and Sybil user votes). This rating will benefit the user to buy the guaranteed and efficient product online.

Some of the challenges to compute are

1) Collecting group information relating to the Sybil activities.
2) Analysing the product voting of the user.
3) Collecting information by the people who don't rate the bought products online.

As a solution to these challenges, a two-line mechanism is proposed here.

A. Definition

Online social networks have variety of users where it is becoming difficult to differentiate between the trusted users and Sybil users. Sybil users on social networks misguide the real users, this would cause trouble to user while sharing their data or while buying product online.

B. Objectives

- Finding the real users in online social networks.
- Computing the TrustRank of the user with the help of Trustrank algorithm.
- Detecting the Sybil communities and colluded votes for a particular product.
- Recommending an efficient and a good rated product to the user online.

C. Assumptions

- All registered users are marked as unknown in their online status.
- No products are available until and unless any user buys the product and rate that particular product online.
- Communities formed online will be of any type irrespective of users.
- All users of Sybil community are treated as Sybil users.
- Each user having more than three negative link sign then we would consider his vote as a Sybil vote.

IV. SYSTEM OVERVIEW

System architecture here is a client server module as shown in Fig.1, where each client is a user and server is the database, MySQL database is used as the server. Users register themselves on online social networks and create their own profiles. Each user profile contains the number of already known friends, friend requests, List of communities they like and etc., Each user online have all the privileges to buy products using the created profiles and rate those bought products online. The registered user of the social network can send the request to another user in order to be friend with the other user. The other user can accept it or reject the request sent. The request interactions of the user are modelled as a friend interaction score. This Scores are plotted as a signed and directed graph G (V.E), where V are the nodes also referred as users on social networks and E are the links between the friend users. With the help of friend interaction online each user TrustRank will be calculated. TrustRank of each user will be accounted for product rating bifurcation.

On the server side, two modules (i.e., System process and general process) are designed. As soon as user get registered, system process generates an authentication code and sends to the user. Each user on receiving the authentication code should enter it on the registration page to get authorised and gain access to profile creation. These details include basic user information like name, date of birth, profession etc., As the user details are entered manually, will be allowed to send or receive the friend request online. Once the sent request is accepted by the other user then the user status will change to trust user. If the sent request is rejected by the other user then the status of the request sent user will be set to Sybil user. If the sent request is pending, then we would not consider it as a trust/Sybil until either of the accept/reject action is performed.

Users registered online and if their status is set to trust then that particular user has permissions to launch the product details that they have bought online. After launching each product user can vote for that particular product and can post a comment (positive/negative). Voted product can be recommended to the other friends as well online. General process module enables each one of them on social networks to view the launched product and can vote for the product. Voting for a product can also be done by the users who have not bought or who have no idea. This kind of user rating product intentionally to make product rating more or to make the rating lesser than the actual rating. This Sybil votes here are considered as colluded votes.

Users on network can view the products launched. Recommending products in online social networks are done by sending the product links to the other users. If a trusted user sends a link to the other user on line, then that is considered as a real link. Sybil user sending a product link to the other user then that link is considered as a Sybil link. Users have no idea while accessing those links about a trusted user product or a Sybil user product. Bifurcation of Sybil and trusted votes are seen only when that product launched is viewed. Based on this votes user can buy a product which is efficient rather than fooling around by buying a fake product online.

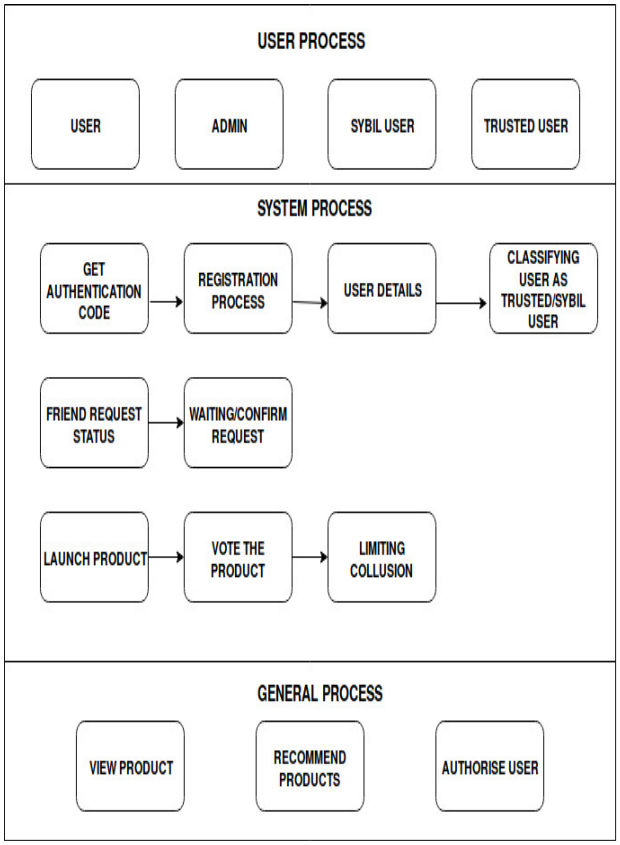

Fig. 1.System Architecture for Product Recommendation

V. SYBIL DETECTION BASED ON PRODUCT VOTING

Individual Sybil detection is important to know the community details of the users interested. This detection is done by the admin by users feedback in the friend interaction mechanism. Vote aggregation of a particular user is taken into account and then checks whether the user is casted his vote on a real user or a Sybil user. The value each vote can be either a positive/negative (link sign). This feedback information of votes will help in reducing collusion of votes on the products in the application. Through this mechanism of vote aggregation and feedback Sybil users are detected. Each user having more than three negative link sign then we would consider his vote as a Sybil vote.

Each node in VoteTrusts have two important features.

1) Vote Capacity: - V(v) is the number of Votes a node v can cast on another node. The maximum number of votes a node can cast is one. This vote value rate if rejected (-1) or accepted (1) depending on the vote is casted.
2) Global Acceptance rate: - P(u) is the positive votes accepted by node u. it indicates the probability of node u is accepted by real user.

A node is considered as Sybil if it has low acceptance rate (i.e., less than the threshold) threshold value here is 0 3. This limits the Sybil collusion in product recommendation.

VI. COMMUNITY STATUS DETECTION

Sybil community detection is done to avoid the users from the same community from voting a product. As the user status is set to trusted/Sybil, admin verifies status of each users online. With this verification system process differentiate between a Sybil user and trust user with the help of TrustRank algorithm. Trusted user status is not targeted. Sybil user status are targeted by the system process and declares those communities as Sybil communities. Sybil community detection algorithm is used to detect the Sybil communities. Input to this algorithm will be the name of the user, community details of the user interested and the status of the user. As the status of the users will already be computed with the help of number of friend requests accepted and rejected this can be used as users profile details. This user list is stored in the database used. From this database results of the user with community names where status of the user is Sybil is fetched executing a Sequence Query Language.

Table- I: Sybil Detection based on Product Voting

Input: Total Votes of Products.
Output: Individual Sybil User.
begin
Step 1: Create a arraylist of users casted vote for particular product with different service providers.
Step 2: Check Ranking of the Products in list
Step 3: Analyse the rank of Product
if (sum of first preferences of Particular product > sum of not first preferences of particular product)
then (max value = sum of first preference of particular product)
else (check for rank of other product)
Step 4: Higher the max value more is the product rank
if (same user found in list of sum of not first preferences of particular product more than 3 times)
then (status = Sybil user)
else (retain previous status of user)
end

Each community names with Sybil users in it are displayed. Sybils displayed can be of type 1 Sybil and type 2 Sybil. Type 1 Sybils are those who are identified as fake users while entering a wrong code during the user registration. Type 2 users are those who has more number of rejection rate than friend request acceptance rate. If type 1 users are found they are termed as Sybil users and type 2 are found, then they are actual Sybils in the application. For every user in the application the iterative process of verifying is carried out. For every n users it is verified whether a Sybil user or trusted user. If Sybil user belongs to a community that particular community all users votes are added into fake vote category, else user is termed as trusted user. Communities without Sybil users are termed as trusted community in OSN.

VII. TRUSTRANK OF THE USER

TrustRank algorithm ranks user depending on the acceptance rate during the friend invitation interaction. Friend invitation interaction is the process of sending or receiving the friend request.

If the friend request sent is accepted, then the accepted request count 1 for that particular user will be one. If the friend request is rejected, then that would count -1 for that particular user. Keep count of all the requests received and rejected user acceptance value is taken into account. User acceptance is the sum of all the accepted request out of number of friend requests sent. The acceptance rate should be always greater than the threshold 0.3. If 0.3 is the user's acceptance rate, products recommended by those users can be chosen to buy products online. If the product recommendations are made by the user with acceptance rate lesser than the threshold, then those votes are added on to the fake vote list.

Table- II: Community Status Detection algorithm

Input: User Details.
Output: Status of Community.
begin

Step 1: Creating array list with username, community and status by the user.

Step 2: Establishing the connection with database and execute the query "select from community table where user status= Sybil and community name".

Step 3: Display the list f Sybils belong to particular community.

Step 4: Establishing the connection with database and execute the query select from community table where usertype 1= Sybil and usertype 2= Sybil and community
name and store into to a list.

Step 5: foreach user n do
if (n is a unauthorised user)
user type=1
else
user type=2
endif
endfor
Step 6: for i = 1 to n do
if ($n_i \in$ SybilCommunity)
Status=Sybil
else
status=trusted
endif
endfor

Step 7: return status
End

Table- III: TrustRank of User

Input: Total friend Request, Accepted Request, Rejected Request and Pending Request.
Output: TrustRank Of User.
begin

Step 1: Create a arraylist of Total request, Accepted request, rejected request, pending request status of usertype1 and usertype 2.

Step 2: set accept rate =0 and Threshold value 0.3;.

Step 3: acceptance rate = $\frac{\text{Accepted request}}{\text{Threshold pending request}}$

Step 4: establish the connection with database and execute the query. Select * from user table where acceptance rate > threshold value and usertype1= Ktrust and usertype 2 = trust order by acceptance rate dese;
end

VIII. RESULTS ANALYSIS

Product recommendations are based on the trusted user votes for a particular user. Methods used for bifurcation of trusted user vote and Sybil votes are analyzed in this section. We have used Amazon product data-set [16] which consists of product id, product ratings and other products purchased together. For number of 1000 users, number of products considered here are 750. The reason to select this data-set is to check the product recommendation accuracy and to determine the number of attack lines from two defense mechanism schemes. The number of votes are determined and further trusted votes and Sybil votes are bifurcated. The difference between the products without bifurcated votes and with bifurcated votes are computed and analyzed. From Fig.2 we can see that the rating for products with analysis of trusted users and fake users are more in number. This actually makes product rating higher for unworthy products. Products recommended are irrespective of whether product is purchased by user.

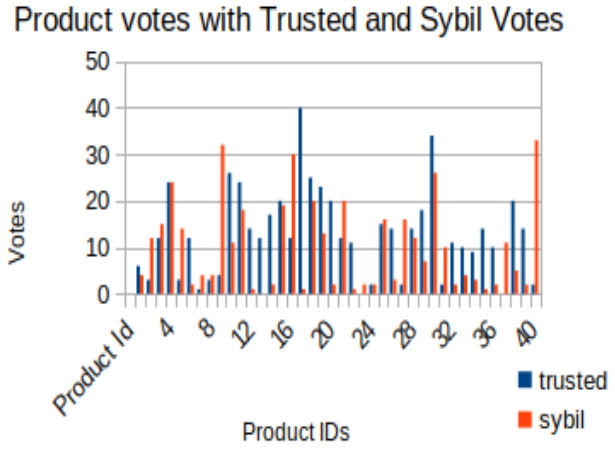

Fig. 2. Product Recommendation

From Fig.2 we can observe that with the help of vote bifurcation each vote to rate product is differentiated and given a worthy value to guide users online regarding efficient products. This implies that using friend interactions online can fetch and recommend a trustworthy product to the user. Complexity of the iterations carried out are overhead because each time a vote is casted each vote has to be verified whether it is voted by a trusted user or Sybil user.

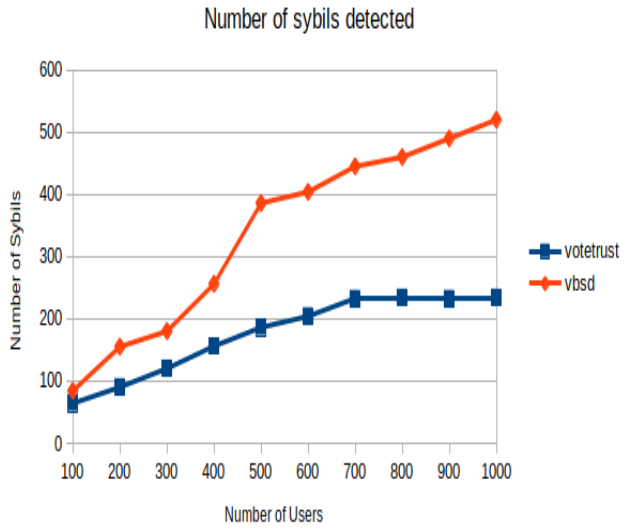

Fig. 3.Sybil detection

Fig.3 shows the number of Sybils that are encountered in the social networking data. The number of Sybils found with the help of vote bifurcation, users termed as Sybils are blocked in the network and then community status detection algorithm is processed. Then the community status of each community detected is retrieved. Now each community turned out to have status Sybil is blocked (i.e., each user in that community irrespective of his individual Sybil status is blocked). By this we can prevent the Sybil accounts that overlap and rate the product multiple times.

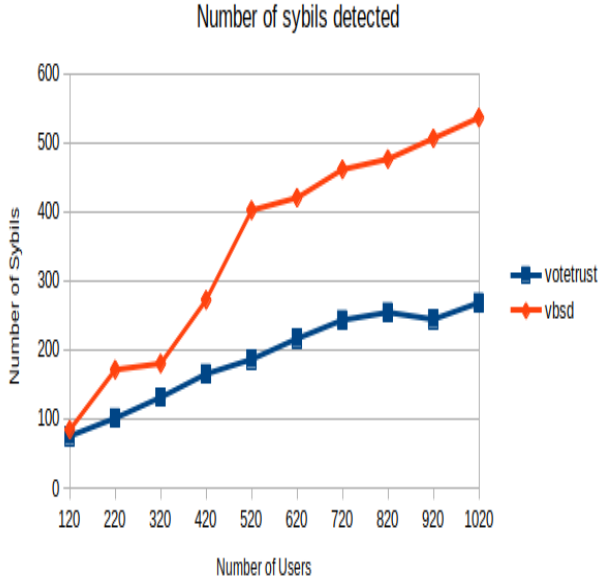

Fig. 4.Sybil Detection after adding Explicit Sybil

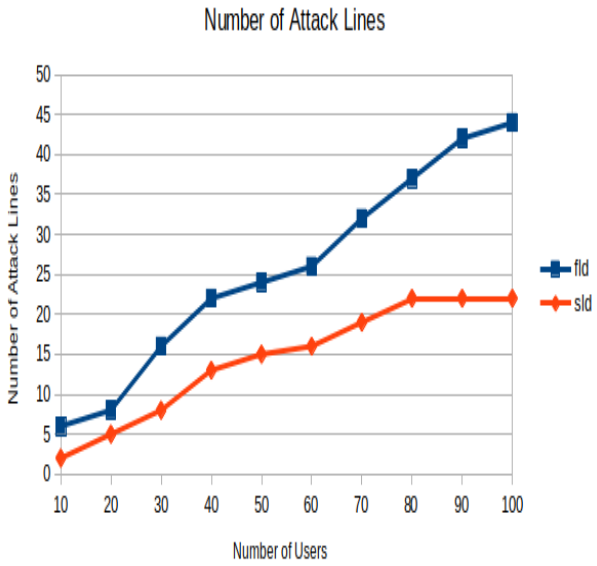

Fig. 5.Defence Line Mechanism

Once after working on the actual dataset we have explicitly added 20 Sybil accounts to check the number of actual Sybil account are revealed are not. Fig.4 shows the number of Sybils that are encountered in the social networking data after explicit addition of 20 Sybil accounts with same basic user details. Sybil accounts more than 15 explicitly added accounts were determined. By this we can tell that Sybil detection is happening with the recommended algorithms and the procedure of the work flow. Tab.IV shows the % of Sybil detection for both VoteTrust and Vote Based Sybil Detection(VBSD). There is increase of 16% Sybil detection in VBSD than VoteTrust and after adding explicit 20 Sybil accounts 31.50% increase in Sybil detection. By this it is determined that VBSD is better than VoteTrust.

Table- VI: PRODUCT RANKING

Data	VoteTrust	VBSD
Actually Data-Set	31.85%	47.44%
Data-Set with explicit Sybils	61.54%	61.54%

To check the number of attack line we have 100 users taken into account. The number of attack lines expected without any defense line mechanism is equal to the number of users registered on social networks. Because each user can either send a positive link or a negative link but not both positive and negative link in the OSN's. First line of defense mechanism(FLD) is avoiding Sybil users during their registration. If the Sybils are not avoided in the first line of registration, then the number of attack line are 46.72% more than the system without avoiding mechanism. Fig.5 shows that the number of attack lines in the system after going through the second line of defense mechanism(SLD). The second line of defense mechanism is avoiding the Sybil communities with the help of Table.II. The number of attack lines are 26.18% lesser than of first line of defense mechanism. From this we can observe that the number of attack line that would occur because of Sybils are reduced and the users are guided with the efficient product results without fooling around themselves in network.

IX. CONCLUSIONS

Sybil attacks are considered as a real challenging problem in OSNs. The proposed system overcomes this challenges by implements Sybil Community Detection algorithm and TrustRank algorithm. Sybil Community Detection algorithm finds each user type (1 or 2), finds the Sybil users. Once Sybil users are detected then that complete community will be treated as a Sybil community and all users inside that community will be treated as Sybil users. With the help of TrustRank algorithm the number of trusted users based on threshold 0.3 are computed and ranked as trusted user or Sybil users. Using these algorithms are benefiting user in finding the efficient product and will not be misguided in purchasing the product online. With bifurcation of votes user has a wider option to think about a product before initiating any action of purchase. This system can be used in any e-commerce site to limit their users on rate without purchasing any of the products. This can be further improved by merging the defence mechanism and avoiding Sybils at the initial stages and decreasing the system overhead and provides more privacy to users.

REFERENCES

1. J. Xue, Z. Yang, X. Yang, X. Wang, L. Chen, and Y. Dai, "Votetrust: leveraging friend invitation graph to defend against social network sybils," in *INFOCOM, 2013 Proceedings IEEE*, pp. 2400–2408, IEEE, 2013.
2. M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within vanet.," *IJ Network Security*, vol. 9, no. 1, pp. 22–33, 2009.
3. N. Z. Gong, M. Frank, and P. Mittal, "Sybilbelief: A semi-supervised learning approach for structure-based sybil detection," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 976–987, 2014.
4. Y. Boshmaf, K. Beznosov, and M. Ripeanu, "Graph-based sybil detection in social and information systems," in Proceedings of the *2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pp. 466–473, ACM, 2013.
5. S. Lv, X. Wang, X. Zhao, and X. Zhou, "Detecting the sybil attack cooperatively in wireless sensor networks," in *Computational Intelligence and Security, 2008. CIS'08. International Conference on, vol. 1*, pp. 442–446, IEEE, 2008.
6. M. Al Mutaz, L. Malott, and S. Chellappan, "Leveraging platoon dispersion for sybil detection in vehicular networks," in *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference*, pp. 340–347, IEEE, 2013.
7. X. Zhang, H. Zheng, X. Li, S. Du, and H. Zhu, "You are where you have been: Sybil detection via geo-location analysis in osns," in *2014 IEEE Global Communications Conference*, pp. 698–703, IEEE, 2014.
8. B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, pp. 1–8, ACM, 2006.
9. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in *ACM SIGCOMM Computer Communication Review*, vol. 36, pp. 267–278, ACM, 2006.
10. B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based sybil defenses," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 363–374, 2011.
11. W. Wei, F. Xu, C. C. Tan, and Q. Li, "Sybildefender: Defend against sybil attacks in large social networks," *in INFOCOM, 2012 Proceedings IEEE*, pp. 1951–1959, IEEE, 2012.
12. A. Cheng and E. Friedman, "Sybilproof reputation mechanisms," in *Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*, pp. 128–132, ACM, 2005.
13. S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th International conference on World Wide Web*, pp. 640–651, ACM, 2003.
14. J. Jiang, C. Wilson, X. Wang, W. Sha, P. Huang, Y. Dai, and B. Y. Zhao, "Understanding latent interactions in online social networks," *ACM Transactions on the Web (TWEB)*, vol. 7, no. 4, p. 18, 2013.
15. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, pp. 35–47, ACM, 2010.
16. J. Leskovec, L. A. Adamic, and B. A. Huberman, "The dynamics of viral marketing," *ACM Transactions on the Web (TWEB)*, vol. 1, no. 1, p. 5, 2007.

AUTHORS PROFILE

Manasa S M is a full time Research Scholar in the Department of Computer Science and Engineering from University Visvesvaraya College of Engineering, Bangalore University, Bengaluru, India. Her research interests are in the field of Social Networks and Web of Services.

Tanuja R is currently the Assistant Professor, Department of Computer Science, University Visvesvaraya College of Engineering, Bangalore University, Bengaluru. She was obtained her Bachelor of Engineering from BMSCE, Bengaluru. She received her Masters Degree in Computer Science and Engineering from UVCE, Bengaluru. Her research interests are in the field of Wireless Sensor Networks, Cryptography and Network security.

Manjula S H is currently working as a Professor, Department of Computer Science and Engineering, UVCE, Bangalore University, Bengaluru. She pursued BE, and M.Tech. in Department of Computer Science and Engineering from UVCE, Bengaluru. Ph.D. in Computer Science and Engineering, Chennai. Her research interests are in the field of Wireless Sensor Networks and Data mining.

Venugopal K R is the current Vice-chancellor of Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science, Bangalore. He was awarded Ph.D in Economics from Bangalore University and Ph.D in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 64 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems etc., He has filed 101 patents. During his three decades of service at UVCE he has over 640 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining. He is a Fellow of IEEE, ACM and ISTE.