MJRET

Open Access

Multidisciplinary Journal of Research in Engineering and Technology

Journal homepage: www.mjret.in

ISSN:2348 – 6953

IDENTIFICATION AND ANALYSIS OF FAKE IDENTITIES ON OSN

Rupali Kate, Jagruti Mahajan, Komal Narke, Priyanka Matere

G. S. Moze College of Engineering Pune, India

Savitaribai Phule Pune University

Abstract : *Online social networking site suffer from the usage of fake accounts that leads to fake product reviews, advertise, malware and spam. Existing system focus on using the social graph approach to detect fakes. However, our project shows that fake user could be friend of a large number of genuine users, invalidating the assumption of social graph based detection. In this project, we represent VoteTrust, a reliable system that further protect user level activities. VoteTrust models the friend request scenario among users as a directed, signed graph, and use two key mechanisms to find fake user over the system : a voting-based fake detection to find users that other users vote to reject, such that fake user community detection to find other colluding fake around identified Sybil's. Through evaluating on social network, we show that VoteTrust is able to prevent user from generating many irrelevant friend requests.*

Keywords: *Global Acceptance ratio, Sybil attacks, social networks, social network-based Sybil defense, Short text classifier, Machine Learning.*

1. INTRODUCTION

Online Social Networks (OSNs) are today one of the greatest popular interactive medium for users to share, data, chat, multimedia and all. But all OSN have big problem of Sybil user on OSN. The Facebook have stated that statistics the average user creates 90 pieces of content per each month, whereas more than 30 billion pieces of content (notes, web links, photo albums, blog posts, news stories, etc.) In Facebook also there are many Sybil creating the account daily.

The aim of proposed system is mainly to provide the OSN without the Sybil user. For that we are using the accept and reject Ratios and Voting Mechanism.

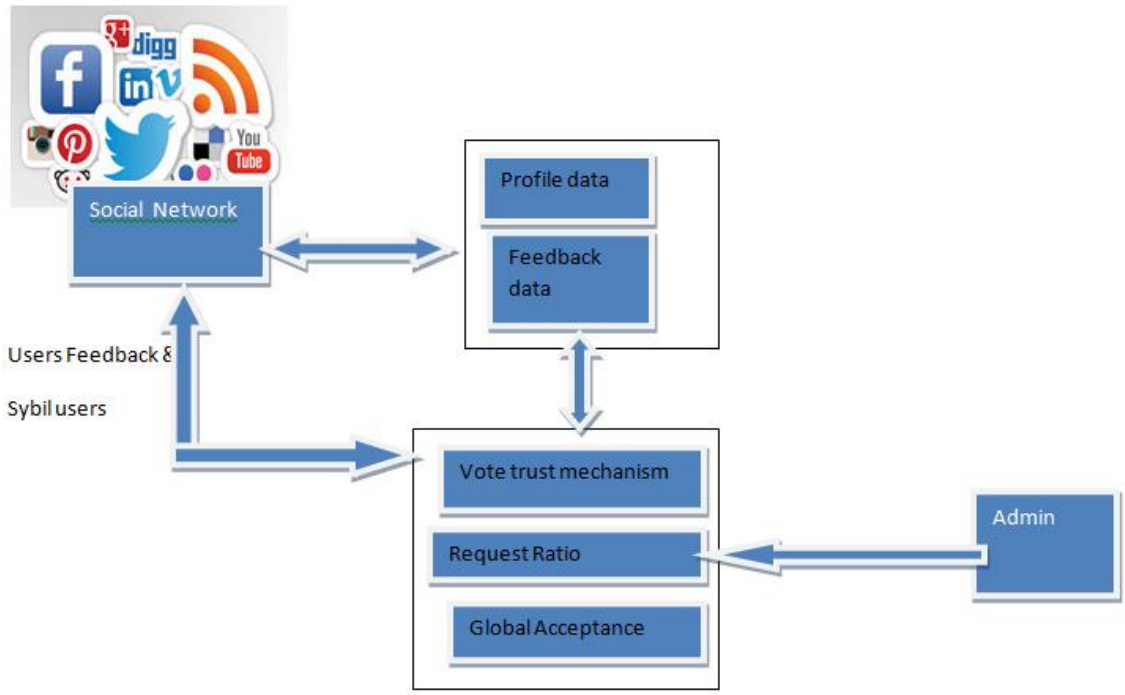


Fig1. Architecture Diagram

In this block diagram we are demonstrating the overall flow of the project implementation idea. Sender is the one who post messages/links or both on the user wall, for that sender should be friend of user. Before posting the post on the user wall, system will check if the user is blocked user or not. If it is the blocked user then the messages, image or links will be discarded and would not reach to the user wall, if it is not a blocked user, the filtering criteria will be applied on the message, images or links.

The main aim of trust-based vote's assignment is to assign low vote capacity to fake users that can be useful to limit the number of votes that fake users could cast for each other. In order to carry out this functionality we first select some trusted users as seeds Vs, and through this seeds propagate the vote capacity to others along the links of friend invitation. As Fake users region has a limited number of in-links we can say that the total vote capacity entering the Sybil region is constrained.

2. RELATED WORK

Sybil attacks has become an increasing pervasive and dangerous problem as more and more people rely on online social networks for online communication and discover realtime information on the Web. For example, according to a report on Facebook in August 2012, there are more than 83 million illegitimate accounts in the social network out of its 955 million active accounts.

- These undesirable accounts are fabricated for various purposes such as spreading malware and spam, or gathering many `likes' from users to unfairly promote

products. Similarly, a lot of fake Twitter followers are sold rampantly in e-markets and bought by people to increase popularity or launch underground illegal activities.

- Besides, an adversary can manipulate Sybil's to conduct malignant activities.

3. EXISTING SYSTEM

To defend against Sybil's, prior Sybil defenses leverage the positive *trust* relationships among users, and rely on the key assumption that Sybil's can befriend only few real accounts. Unfortunately, we find that people in real OSNs still have a non-zero probability to accept friend requests of strangers, leaving room for Sybil's to connect real users through sending a large amount of requests.

4. PROPOSED SYSTEM

In this, we further explores the negative *distrust* relationships (e.g., in the form of rejected friend requests) among users, as Sybil's have more distrust relationships than trust ones with real users. However, this feature cannot be directly applied because attackers could obfuscate their Sybil's from the detector by generating many fake trust relationships among Sybil's.

To prune the fake relationships, we model the friend invitation interactions among users as a signed, directed network, with an edge directed from the sender to the receiver and a sign (1= ¡ 1) indicates whether a friend request is accepted.

Based on the above rationale, we present *VoteTrust*, a system that leverages the friend invitation graph to detect Sybil's. In VoteTrust, we say that a node B casts a (positive/negative) vote on a node A if B accepts/rejects the request from A. VoteTrust first uses a PageRank style algorithm to appropriately assign the number of votes that one can cast on another node (referred to as *vote capacity*).

This process assigns few vote capacity for individual Sybil's and thus prevents them from significantly vouching each other through collusion. After that, VoteTrust evaluates a *global* acceptance rate (i.e., the probability of being a real user) for each node through aggregating the votes over the network. During the aggregation, VoteTrust further penalizes votes from suspected nodes. Due to more negative votes from real users, Sybil's would get low global acceptance rates and thus can be identified out.

5. MATHEMATICAL MODEL

VoteTrust models the friend invitation interactions among users as a directed, signed graph to detect Sybil's over the graph: a voting-based Sybil detection to find Sybil's that users vote to reject, and a Sybil community detection to find other colluding Sybil's around identified Sybil's.

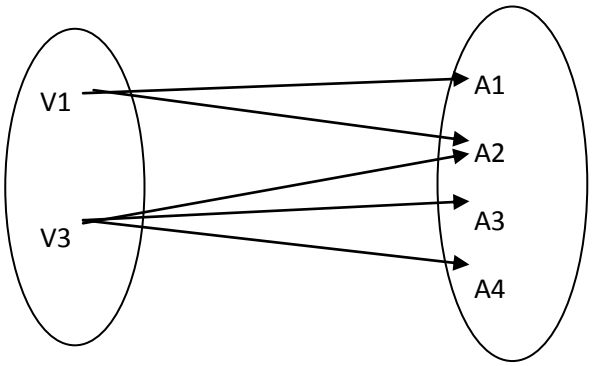
Consider a set V, A set of users registering with our system. This set can be represented as follows :

V= {V1, V2, V3,….VN}

These users can perform social activities such as chatting, profile update, add remove friends, search friends etc. Now consider a set a which is a set of social activities, user can perform. This sent can be represented as,

A = {A1, A2, A3…An}

The relation between these two sets can be represented as follows. It shows the one to many relationship, that is a user can perform multiple social activities.



The main aim of VoteTrust is to takes as input the friend invitation graph *G*, and outputs the classification of any node or user *u as real*, *Sybil* or *unknown*.

The friend invitation graph G is represented as follows:

G = {V, E}

Where V – Set of nodes or users
E – Represented the set of links

A link *e* = (*u, v, s*) from *u* to *v*, of sign *s* = 1, indicates that *v* trusts *u* and accepts its request. If *s* = -1, then *v* distrusts *u* and rejects its request.

There are two methods that we are working on here in order to detect Sybil's from social network. First is Trust based vote assignment and second is Global Vote Assignment.

In first method the friend invitation graph is used in order to detect the Sybil users. Here we first select some trusted users as seeds, and then propagate the vote capacity from the seeds to others along the links of friend invitation graph *G*(*V;E*).

As Sybil region has a limited number of in-links, the total vote capacity entering the Sybil region is constrained. The initial vote capacity of user u is represented as follows:

$$\boldsymbol{I(u) = \frac{N}{Vs} \ \ If (u€Vs)}$$

Where N – Total vote capacity of system.
Vs – Trusted seeds, we equally assign the vote capacity over *Vs.*

In second method global vote aggregating is done to get the global acceptance rate *p*(*u*) of a node *u*.
As the acceptance rate of sybil's is very low as compared to real users. SO we can use this two methods to detect sibyls from social network.

6. ALGORITHAM

VOTETRUST-D(G; Vs)

- *if u* $\boldsymbol{\epsilon}$ *Vs then* *vote assignment*
  I(u) $\leftarrow$ *N=*$|$ *Vs*$|$
- *else*
  I(u) $\leftarrow$ *0;*
- *end if*
- *while* $\Delta >$ $\boldsymbol{\epsilon}$*1 do*
- *for u* $\boldsymbol{\epsilon}$ *V do*
- $\mathrm{U}(u) = d.\sum_{v:(v,\mathcal{U})\epsilon E} \frac{\vartheta(v)}{\omega(v)} + \big((1-d).I(u)\big)$
- *end for*
- *end while*
- *p(0)* $\leftarrow$*0:5;* *vote aggregating*
- *while* $\Delta >$ $\boldsymbol{\epsilon}$*2 do*
- *for u 2*$\boldsymbol{\epsilon}$ *V do*
- *P(u)=* $\frac{\sum v:(v,\mathcal{U})\epsilon E+\vartheta(v).p(v)}{\sum v:(v,\mathcal{U})\epsilon E\vartheta(v).p(v)}$
- *p* $\leftarrow$*WilsonScore();*
- *end for*
- *end while*
- *end procedure*

7. CONCLUSION

1) Provide the security guarantees of VoteTrust, demonstrating that we limit the number of requests Sybil's can send to real users.

2) First, we introduce a new graph model for Sybil defense, which nicely combine link structure and user feedback.

3) Second, we propose new techniques, including global vote aggregation and local community expansion, to exploit the negative links. Finally, we present and analyze theoretically the security guarantees of VoteTrust.

REFERENCES

[1] K. Thomas, C. Grier, D. Song, and V. Paxson, "Suspended accounts in retrospect: an analysis of twitter spam," in Proc of IMC '11, New York, NY, USA, 2011, pp. 243–258.

[2] G. Stringhini, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Zhao, "Follow the green: Growth and dynamics in twitter follower markets," in ACM Internet Measurement Conference (IMC), 2013.

[3] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai,"Uncovering social network sybils in the wild," in Proc. of IMC,2011.

[4] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in Proc. ofSIGCOMM, 2006.

[5] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding thedetection of fake accounts in large scale social online services,"in nsdi, 2012.