VoteTrust: A System to Defend against Social Network Sybils in Facebook

Priyanka
M.Tech student
Dept of ISE,
MSRIT, Bangalore

Deepthi K.
Assistant Professor
Dept of ISE,
MSRIT, Bangalore

ABSTRACT

The Sybil attack is one where an user creates multiple Duplicate or fake identities to compromise the running of the system. Online social networks(OSN) suffers from the creation of fake accounts that introduce fake product reviews, malware and spam, existing defenses focus on using the social graph structure to isolate fakes. This paper presents VoteTrust- a salable defense system that further leverages user level activities. VoteTrust models the friend invitation interactions among users as a directed, signed graph, and it uses a Sybil detection algorithm to find Sybil users, who have more chances of rejecting friend request than normal users. Facebook operates a leading real-name social networking internet platform, which enables users to connect and communicate with each other, share information, and to enjoy a wide range of other features and services. Through evaluating Facebook social network, it can be shown that VoteTrust will able to prevent Sybil users from generating many unsolicited friend requests.

General Terms

Facebook, Sybil user

Keywords

Online social networks(OSN), Security, Sybil attack, Sybil detection, Unsolicited friend requests.

1. INTRODUCTION

It is a dangerous digital world out there, Security for software or an application is important for any network. One way security can break down is in a Sybil attack, it was named after the case study of a woman with multiple personality disorder, a Sybil attack is a type of security threat when a node in a network claims multiple identities[1].

The term sybil refers to the person who acts moody and irregular. It can be self described as feeling of being “not quite oneself”. Sybil attack is one where a single user pretends many fake or sybil identities who creates multiple accounts from different IP addresses.A sybil user can be distinguished by observing their behavior through the VoteTrust algorithm[2]. The social media sites have changed the way one interact with each other[5]. Sites like Facebook, Twitter, LinkedIn, and more made our life simple to stay connected in peoples lives. Facebook allows users know their business more intimately[1, 7], Through these sites one can communicate through status updates, photos, messages and more. With Twitter, one can share news and updates about our business quickly, By including false information by the Duplicated entities, an user can mislead a system into making decisions benefiting. For example, in a distributed review system, an user can easily change the overall review option by providing many false reviews, the using fake identities hence defending against Sybil attacks is quite challenging[4].

1.1 Scenarios of Sybil Attack

There are Different scenarios in which Sybil Attack occurs are enlisted below.

(1) Routing in a Distributed Peer-to-peer System: To improve the performance, wireless networks usually adopt a multi-path routing technique. Instead of using a single routing path, multipath routing is used throughout a network [2, 8].
(2) Voting Applications in Peer-to-peer: Most of the voting systems assume that each user has one identity, and by using that identity a user can provide only one vote, if attacker has multiple identities than user can have multiple votes.For example, Flipkart’s user feedback system is essentially a grouping voting system, since the reputation of each merchant is determined by the votes from customers[3].
(3) Sock puppets in Online review Forums: Sock puppets are used in order to cheat people on the Internet. For example, to believe that a product is a good buy, a usual plan is to use different duplicate online identities pretending to be different people. This is done to increase the value of for the product[6].

1.2 Methods to defend sybil attack

There are different methods to defend sybil attack, they are enlisted below.

(1) Trusted certification: Here central authority, will verify the validity of each user and issues the certification to hostel one by verifying contact no, Email Id, etc.
(2) Registration Fee: Add an economical fee with each certification, attackers cannot easily join and they cannot affect system unless they spend a lot of money.[6].

To defend against Sybils, prior Sybil defenses leverage the positive trust relationships among users, and rely on the key assumption that Sybils can befriend only few real accounts. But, we find that

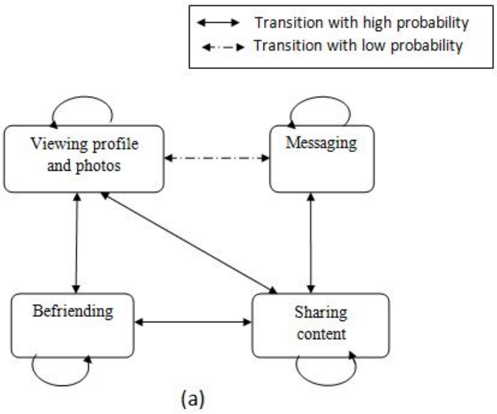
Transition with high probability
Transition with low probability
Viewing profile and photos
Messaging
Befriending
Sharing content
(a)

Fig. 1. (a) State transitions for a Sybil user.

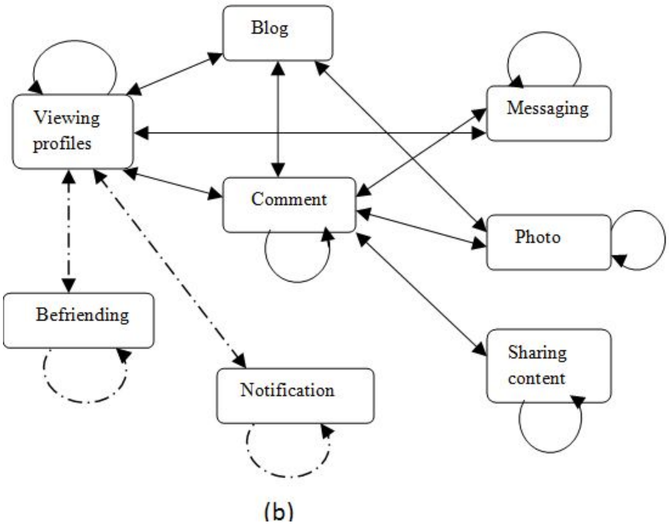

Fig. 2. (b) State transitions for a normal user.

people in real OSNs still have a non- zero probability to accept friend requests of strangers, who are allowing Sybils to connect real users through sending a large amount of requests. OSNs further explores the negative distrust relationships (e.g., in the form of rejected friend requests) among users, as Sybils have more distrust relationships than trust ones with real users[12]. The behavior of real and the sybil user can be explained by using transition diagram in figure 1 and figure 2 respectively.[14].

Consider a social network Facebook that adopts a friend request/confirm mechanism. One has to send a request in order to befriend another user, and the recipient can accept or reject the request[11].

What is the key difficulty of Sybils?

The key difficulty of Sybils is to befriend many real users. However, Sybils can easily overcome this difficulty by sending a large amount friend requests[13].

Can we directly use this difficulty to detect Sybils?

We detect Sybils with number of friend requests, user may accept or reject request. One Sybil can send friend requests to other colluding Sybils, who are guaranteed to accept these requests.

2. SYSTEM MODEL

2.1 Befriending Behavior of Sybils

Friend invitation graph: a directed and signed graph G(V,E), where V is set node and E is links. Friend invitation graph and the structure of Sybil community is shown in figure 3. 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.

Where u $\rightarrow$ (0)$\{$Sybil users community$\}$ and $\rightarrow\{$Normal users community$\}$ [15].

To appear as real to the system, an attacker could create many positive links among Sybils. The objective of the attacker is create as many links as possible with the real region. Attack-link is used to represent the link that goes from the Sybil region Gs to the real region Gh[13].

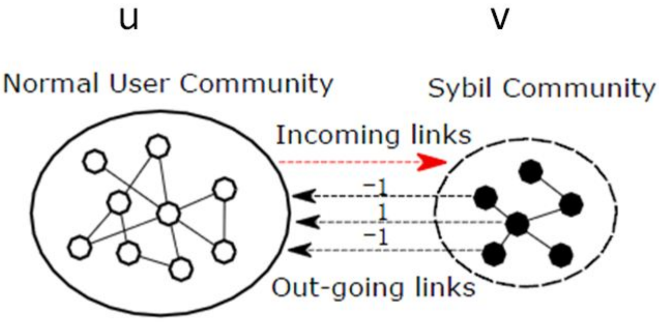

Fig. 3. Illustration of the friend invitation graph and the structure of Sybil community.

2.2 The goal

Goal of VoteTrust is to take many users of application, and outputs the classification as w →{real, Sybil or unknown} $\forall w \in V$. Where V is the set of nodes and w is a node that belongs real, sybil or unknown user of the application.
When a node w joins the network, its initial state is unknown, as the node repeatedly sends requests to normal users, then admin can eventually classify it as Sybil or real[9].

2.3 Trust based vote assignment

The main aim of trust-based Votes 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. Select some trusted users as seeds Vs, and vote capacity to others along the links of friend invitation graph G(V;E). 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.

2.4 Global Weight Aggregating

The first method of Vote assignment gives low vote capacity to not only Fake users but also non-popular real users with few incoming links. So to overcome this we introduce the global vote aggregating phase to get the global acceptance rate p(u) of a node u.
In this method, the graph leverages the sign of outgoing links (i.e, the user feedback) for higher accuracy. Fake users have a higher percentage of negative links to real region so we can identify the fake users.

2.5 System Architecture of VoteTrust

VoteTrust architecture consists of user process, system process and general process. User process consists of users of the application, admin who is maintaining the application, and intruder who always tries to distract or attack the system. System process consists of registering for the application, in case of new users. Registered users are going to login into the application, admin can check the user details, Fig 3. shows System architecture of VoteTrust model, which can be discussed as follows.

—System architecture of VoteTrust which shows user process, system process and a general process which can be adopted by both user and admin.

—User process shows admin, users, intruder1, intruder2.

—In the System process, a new user going to register for the application, if new request comes from the unknown user in Facebook application, than the Request status is shown in his homepage, the user can accept friend request or reject. Based on acceptance or rejectance by the user weightage calculation will be done.

—After the weightage calculation, Sybil detection of VoteTrust Algorithm is applied.

—VoteTrust algorithm will calculate malicious user, than the admin will block malicious user, and the details of the malicious user is stored in user process.

—General process of VoteTrust includes uploading of the posting, view of posting, managing of the user groups and managing the statistics of the sybil users.

3. THE PROPOSED ALGORITHM OF VOTETRUST

The VoteTrust approach is described through an algorithm shown below which has two phases Vote Assignment and Vote Aggregating[10].

```
if u Vs then ;**vote assignment**
I(u)←N=| $Vs$|//initial vote capacity of the user u, votes Vs, N=no of votes
else
I(u) ←0;
end if
while $\Delta > 1$ do //if there are more no of users
for u 2 V do
end for
end while

p(0) ←0.5 ;**vote aggregating** // probability of acceptance of user
while $\Delta > 2$ do
for u 2 V do
P←WilsonScore(p)
end for
end while
end procedure
```

3.1 Sybil detection algorithm of VoteTrust will be used to know the status of users

(1) UserId: It is unique user Id given to all users of the application.
(2) Name: It is the name user which one need to mention during registration
(3) Total requests: It is the total no of requests sent by the users to make friends, here in the Facebook application a user sends request in order to be friend with other.
(4) Accepted requests: It is the total no of accepted requests by the user who will receive friend request from other users.
(5) Rejected requests: It is the total no of requests rejected by the user who will receive friend request from other users.
(6) Pending requests: It is the total no of pending requests which the user kept, he may accept friend request later on.
(7) Rejected ratio: It is the ratio of rejected requests to the total requests.
(8) Pending ratio: It is the ratio of pending requests to the total requests.

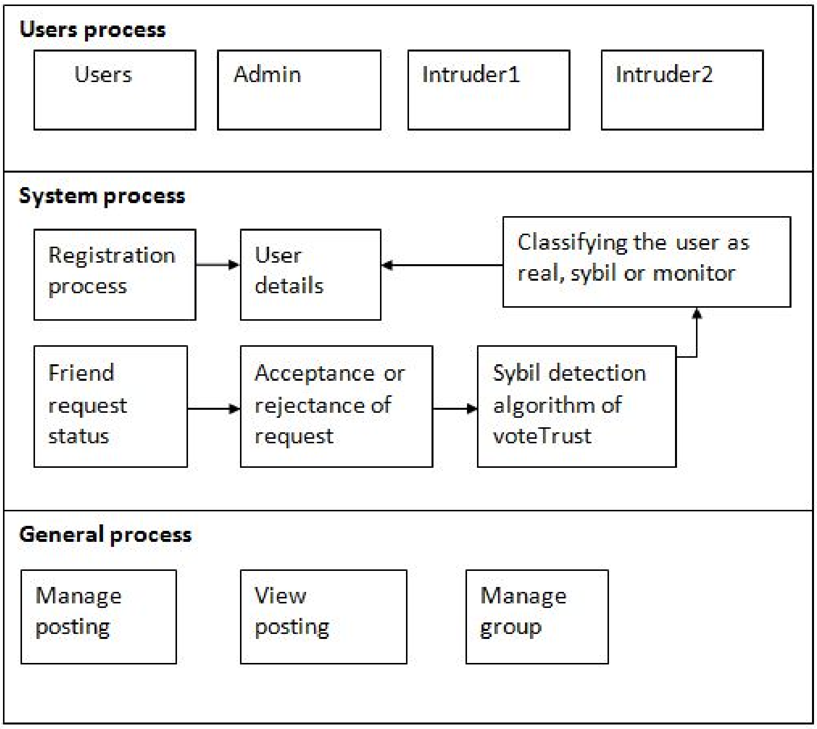

Fig. 4. System Architecture of VoteTrust.

Table 1. Categories of users in Facebook application

Status of users	Features	Behavior
General or real	accept less no of friend requests	will share, comment and view profile
Sybil or Fake	tries to connect with normal users and generate more requests	accept the friend requests faster than normal users
Monitor	keep the requests in the pending state	may accept friend request after some time, admin can't categorize these users as normal or Sybil uses

(9) Status of users: The status of the users may be general(for normal user), Sybil(for fake user) or in monitor state(for the one whose requests are pending), their features and behavior is shown in Table 1.

3.2 Algorithm to know the Status of users

(1) step1: create array list with Total requests, Accepted requests, Rejected requests, Pending requests, Rejected ratio, Status of users.

(2) step2: set rejection percentage=0; pending percentage=0; total percentage=0.

(3) step3: Establish the connection with database, and execute query select * from status table.

```
//loop to know about all users who are in monitoring state
if(rejected requests> 0)
{
rejection percentage=rejection ratio * 100/total requests
pending percentage=pending requests * 100/total requests
}
total percentage = rejection percentage + pending percentage;
```

4. EXPERIMENTAL RESULTS

The objective of this system is to show how to give more security on social network site from the Sybil Attack (Unauthorized users account)and to show how securely one can use facebook and to protect themselves with sybils. From the experimental results one can conclude the rate of sybil accounts in our Facebook application, this application takes take different users, and outputs the classification of any users u, i.e., u→real, Sybil or unknown.

Steps for running VoteTrust web application in Eclipse

(1) Installing jdk
(2) Eclipse installation
(3) MySQL database connection
(4) Tomcat server connection

Table 2 shows sample data set of differnt type of users with userId, name, etc. Based on the acceptance and rejectance request VoteTrust algorithm classify the users, users of the application can block or delete the user information, will calculate malicious user, than the admin will block malicious user, and the details of the malicious user is sent to the admin.

5. CONCLUSION AND FUTURE WORK

Sybil attack is widely considered as a real and challenging problem in online social networking. Sybil attacks in Facebook application

Table 2. Classification of users with VoteTrust algorithm

UserId	Name	Total requests	Accepted requests	Rejected requests	Pending requests	Rejected ratio	Pending ratio	Status of users
1	vijay	4	4	0	0	0	0	General or real
2	Shiva	5	1	4	0	80.0	0.0	Sybil or fake
3	Pooja	5	0	2	3	40.0	30.0	Unknown
4	Divya	2	1	1	0	50.0	50.0	General

will provide the security, by evaluating the VoteTrust, application is able limit the number of requests Sybils can send to real users. Based on acceptance or rejectance by the user weightage calculation can be done. After the weightage calculation, Sybil detection of VoteTrust Algorithm is applied. Hence it will be effective in finding real, Sybil or unknown users. VoteTrust application will take different users as input, and outputs the classification of any users u, i.e., u→{real, Sybil or unknown}. VoteTrust is able to block or delete malicious users on Facebook.

The application can be used more effectively by taking real time data from Facebook, it will helpful to calculate the percentage of real and fake users in Facebook.

6. REFERENCES

[1] why social media is important.

[2] John R Douceur. The sybil attack. In *Peer-to-peer Systems*, pages 251–260. Springer, 2002.

[3] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru. A survey of attack and defense techniques for reputation systems. *ACM Computing Surveys (CSUR)*, 42(1):1, 2009.

[4] Andreas M Kaplan and Michael Haenlein. Users of the world, unite! the challenges and opportunities of social media. *Business horizons*, 53(1):59–68, 2010.

[5] Haewoon Kwak, Changhyun Lee, Hosung Park, and Sue Moon. What is twitter, a social network or a news media? In *Proceedings of the 19th international conference on World wide web*, pages 591–600. ACM, 2010.

[6] Brian Neil Levine, Clay Shields, and N Boris Margolin. A survey of solutions to the sybil attack. *University of Massachusetts Amherst, Amherst, MA*, 2006.

[7] Daniel Nations. n.d. ”what is social media? what are social media sites?”.

[8] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pages 259–268. ACM, 2004.

[9] Al-Sakib Khan Pathan. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2010.

[10] Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. Detecting spammers on social networks. In *Proceedings of the 26th Annual Computer Security Applications Conference*, pages 1–9. ACM, 2010.

[11] Jilong Xue, Zhi Yang, Xiaoyong Yang, Xiao Wang, Lijiang Chen, and Yafei Dai. Votetrust: Leveraging friend invitation graph to defend against social network sybils. In *INFOCOM, 2013 Proceedings IEEE*, pages 2400–2408. IEEE, 2013.

[12] Z. Yang, J. Xue, X. Yang, X. Wang, and Y. Dai. Votetrust: Leveraging friend invitation graph to defend against social network sybils. *Dependable and Secure Computing, IEEE Transactions on*, PP(99):1–1, 2015.

[13] Zhi Yang, Christo Wilson, Xiao Wang, Tingting Gao, Ben Y Zhao, and Yafei Dai. Uncovering social network sybils in the wild. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 8(1):2, 2014.

[14] Kuan Zhang, Xiaohui Liang, Rongxing Lu, and Xuemin Shen. Sybil attacks and their defenses in the internet of things. *Internet of Things Journal, IEEE*, 1(5):372–383, 2014.

[15] Xiaokuan Zhang, Haizhong Zheng, Xiaolong Li, Suguo Du, and Haojin Zhu. You are where you have been: Sybil detection via geo-location analysis in osns. In *Global Communications Conference (GLOBECOM), 2014 IEEE*, pages 698–703. IEEE, 2014.