DETECTION AND BLOCKING OF SYBILS USING VOTE TRUST IN ONLINE SOCIAL NETWORKING

R.Uma,
Assistant Professor,
Saranathan College of Engineering,
Trichy, India.

G.Kiruba,
B.Tech (IT) Student,
Saranathan College of Engineering,
Trichy, India.

D.Devi,
B.Tech (IT) Student,
Saranathan College of Engineering,
Trichy, India.

D.Selvamani,
B.Tech (IT) Student,
Saranathan College of Engineering,
Trichy, India.

B.Vaishnavi,
B.Tech (IT) Student,
Saranathan College of Engineering,
Trichy, India.

Abstract: Unscrupulous users increasingly find Online Social Networking (OSN) platforms as lucrative targets for malicious activities, such as sending spam and spreading malware. The profitability of such activities and the fact that a large portion of the OSN communication takes place over symmetric social links. Unwanted friend requests in online social networks (OSNs), also known as friend spam, are among the most evasive malicious activities. Friend spam can result in OSN links that do not correspond to social relationship among users, thus pollute the underlying social graph upon which core OSN functionalities are built, including social search engine, ad targeting, and OSN defense systems. To effectively detect the fake accounts that act as friend spammers, we propose a system called vote trust. It systems from the observation on social rejections in OSNs, i.e., even we will maintained fake accounts inevitably have their friend requests rejected or they are reported by legitimate users. Our key insight is to partition the social graph into two regions such that the aggregate acceptance rate of friend requests from one region to the other is minimized. This design leads to reliable detection of a region that comprises friend spammers, regardless of the request collusion among the spammers. Meanwhile, it is resilient to other strategic manipulations. Then extend the project to protect the image piracy using water marking techniques in online social networks.

KEYWORDS:-
Online social network, Sybil attack, Sybil detection, Sybil block, Spam.

I.INTRODUCTION

Recently, OSNs have come under Sybil attacks in this attack; a malicious user creates multiple fake identities, known as Sybils, to unfairly increase the power and influence within a target community. Sybil forwarding spam and malware on Facebook and twitter. The profitability of such activities and the fact that a large portion of the OSN communication takes place over symmetric social links motivate attackers to connect to real users. In particular, Attackers leverage the open nature of OSN and send to legitimate users unwanted friend request, also known as friend spam.

To defend against Sybils, prior Sybils defenses leverage the positive trust relationship among users, and relay on key assumption that sybils can be friend only few real accounts. Unfortunately, we find that people in real OSN still have a non-zero probability to accept friend request ofstrangers, leaving roomfor sybils to connect real users through sending a large amount of request.

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

To prune the fake relationship, 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. In friend invitation graph the Sybils has a large number of outgoing links than normal users. We present Vote trust, a system that leverages the friend invitation graph to Detect Sybil. In Vote trust ,we say that a node B casts a (positive/negative) vote on a node A if B accepts/rejects the request from A. Vote trust 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 sybils and thus prevents them from significantly vouching each other through collusion. After that, Vote trust 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, Vote Trust further penalizes votes from suspected nodes. Due to more negative votes from real users, Sybils would get low global acceptance rates and thus can be identified out and blocked.

We provide an image piracy based on water marking approach so that image can be only viewed cannot be downloaded.

II.EXISTING SYSTEM

It uses social-graph-based approach (it implement the protocol that leverage the social graph structure to defend against Sybil). Reputation system using Eigen trust(it is an algorithm where each peer in network a unique global trust value based on peer history uploads and aim to reduce the number of inauthentic files in peer2peer network) to detect the sybil attacks. It uses a Bayesian filters (it is a method to detect the spam) and SVMs (support vector machine, data used for classification and data analysis) are used as feature based approaches to classify the real users.

III.PROPOSED SYSTEM

Implement vote trust that one node casts a certain number of votes for the other. The vote value is determined by the sign of link. DWT (Discrete wavelet transform) algorithm to provide watermark to each uploaded images.

ADVANTAGES:-

- It provides the security guarantees of vote trust
- High precision value(level of measurement that yields consistent results) can be achieved
- Implement large scale environments
- Inexpensive and low complexity system

IV.SOCIAL NETWORK

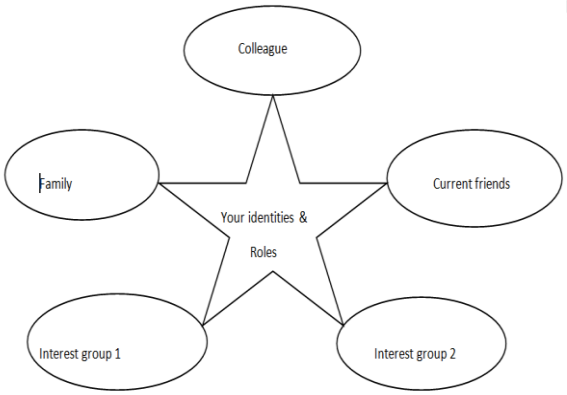

Figure 1

In the figure 1 describe the role of each user in online social networking. Normal user have common relation with other users like family, colleagues, current friends, old friends and some interest groups.

V.SYBIL DETECTION

To limit the Sybil collusion, vote trust uses two key techniques, trust based vote assignment and global vote aggregating, to assign the vote capacity and to properly compute the global acceptance rate.

GLOBAL ACCEPTANCE RATES:-

It is the fraction of positive votes that vote aggregates for a node u, indicating that probability that u is accepted by real users. Node with low global acceptance rate or detected as sybils vote trust uses collision vote trust uses key techniques, trust based vote assignment and global vote aggregation to properly assign the vote capacity and to compute the global acceptance rate.Number votes that Sybils could cast for each other. To achieve this goal, we first select the trusted user as seed and then propagate the vote capacity from the seeds to others along the links of friend invitation graph G(V,E) ,where V and E are the set of nodes and links respectively. As Sybil region as a limited number of inlinks. The total vote capacity entering the sybil region is constrained.

TRUST BASED VOTE ASSIGNMENT:-

The goal of trust based vote assignment is to assign low vote capacity to Sybils show that we can limit the number votes that Sybils could cast for each other. To achieve this goal, we first select the trusted user as seed and then propagate the vote capacity from the seeds to others along the links of friend invitation graph G(V,E) ,where V and E are the set of nodes and links respectively. As Sybil region as a limited number of inlinks. The total vote capacity entering the Sybil region is constrained.

GLOBAL VOTE AGGREGATION:-

Vote assignment gives low vote capacity to not only Sybils but also non popular real users with few incoming links. We thus introduce the global vote aggregating phase to get the global acceptance rate P(u) of a node u. this phase further leverages the sign of outgoing links (i.e., the user feedback) for higher accuracy, as sybils have a higher percentage of negative links to real region.

VI.SYBIL BLOCKING:-

After detecting the Sybil it is blocked automatically. While server processing the friend request the confirm button is disabled

VII.ARCHITECTURE DIAGRAM

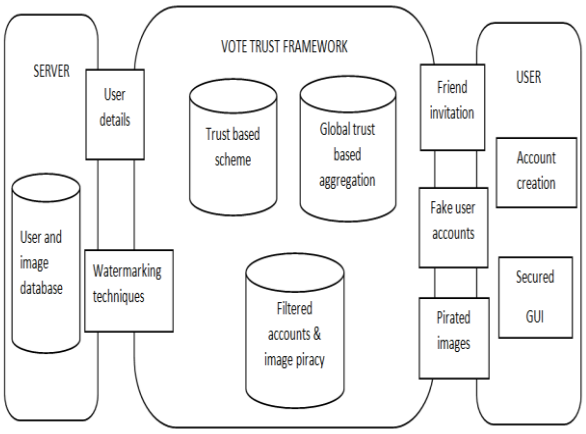

Figure 2

The user details and image are send to vote trust framework contain trust based scheme, global trust based aggregation, filtered accounts and image piracy.

VIII.ROLE OF SERVER

When the user sends the friend request to other user, the friend request also send to the server. The server process the friend request using the vote trust framework. If it is a sybil, the request is blocked by the server and the friend request is invisible to the user. We can provide image piracy using digital watermarking which is the process of embedding a persistent digital identity into images. A digital watermark contains imperceptible digital information, also called its payload, which can be included in anything users choose.

IX.CONCLUSION

We prevent the user from the Sybil and provide secure trust users so that many activities like anti –bulling and spam message can be avoided. The Sybil is detected and blocked using vote trust framework. The image is protected by watermarking approach.

X.REFERENCES

[1].B. Gibbons, and A. Flaxman, "Sybil guard: defending against Sybil attacks via social networks," in Proc. Of SIGCOMM, 2006.

[2] J. R. Douceur, "The Sybil attack," in Proc. of IPTPS, March 2002.

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

[4] H. Gao, J. Hu, Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in Proc. of IMC, 2010.

[5] C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: the underground on 140 characters or less," in Proc. of CCS, 2010.

[6] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybil guard: defending against Sybil attacks via social networks," in Proc. Of SIGCOMM, 2006.

[7] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybil limit: A near-optimal social network defense against Sybil attacks," in Proc. of IEEE S&P, 2008.