

# Votetrust: Strengthening the online social network

Miss. Sushma Torvi, Miss Pallavi koli

**Abstract**— Online social networks (OSNs) are popular collaboration and communication tools for millions of users and their friends. Unfortunately, in the wrong hands, they are also effective tools for executing spam campaigns and spreading malware. Intuitively, a user is more likely to respond to a message from a Facebook friend than from a stranger, thus making social spam a more effective distribution mechanism than traditional email. In fact, existing evidence shows malicious entities are already attempting to compromise OSN account credentials to support these “high-return” spam campaigns. Recently, there has been much excitement in the research community over using social networks to mitigate multiple identity, or Sybil, attacks. A number of schemes have been proposed, but they differ greatly in the algorithms they use and in the networks upon which they are evaluated. As a result, the research community lacks a clear

**Index Terms**— online social network(OSN)..

## I. INTRODUCTION

Avoiding multiple identity, or Sybil, attacks is known to be a fundamental problem in the design of distributed systems. Malicious attackers can create multiple identities and influence the working of systems that rely upon open membership. Examples of such systems range from communication systems like email and instant messaging to collaborative content rating, recommendation, and delivery systems such as Digg and Bit Torrent. Traditional defenses against Sybil attacks rely on trusted identities provided by a certification authority. But requiring users to present trusted identities runs counter to the open membership that underlies the success of these distributed systems in the first place.

All social network-based Sybil defense schemes make the assumption that, although an attacker can create arbitrary Sybil identities in social networks, he or she cannot establish an arbitrarily large number of social connections to non-Sybil nodes. As a result, Sybil nodes tend to be poorly connected to the rest of the network, compared to the non-Sybil nodes. Sybil defense schemes leverage this observation to identify Sybils. They use various graph analysis techniques to search for topological features resulting from the limited capacity of Sybils to establish social links. The literature on Sybil defense schemes is still in its early stages; most papers describe new algorithms, but none provide a common insight that explains how all of these schemes are able to detect Sybils. Each

algorithm has been shown to work well under its own assumptions about the structure of the social network and the links connecting non-Sybil and Sybil nodes. However, it is unclear how these algorithms would compare against each other, on more general topologies, or under different attack strategies. As a result, it is not known if there exist other (potentially better) ways to mitigate Sybil attacks or if there are fundamental limits to using only the structure of the social network to defend against Sybils.

## II. RELATED WORK

H.Gao et.al, proposed in the work, “Detecting and characterizing social spam campaigns” in *Proc. of IMC*, 2010[1]. This system uses IP addresses as identity. The malicious users can readily steal IP addresses. A malicious user can also co-opt a large number of end-user machines, creating a Botnet of thousands of compromised machines spread throughout the Internet. Botnets are particularly hard to defend. Jing Jiang, et.al, in the work, “Detecting and Validating Sybil Groups in the Wild 2012”[2]. Sybil users alone do not harm the system. What is really dangerous is that multiple sybil users collude together and form a sybil group. Advantages of this work is the first attempt to identify and validate sybil groups in Renren online social network. They build sybil group detector based on multiple attributes. The used algorithms are sybil group detector, validation methodology. Amit A. Amleshwaram, et.al, in the work, “CATS: Characterizing Automation of Twitter Spammers” 2013[3]. In this work, they propose several novel features capable of distinguishing spam accounts from legitimate accounts. Feature computation has low latency and resource requirement making fast detection feasible. Used algorithm is clustering algorithm. In this work spammers are not distinguish them from legitimate users. Guangchi Liu, et.al, in the work, “Uncovering the Mystery of Trust in An Online Social Network” 2015[4]. In this work they proposed the properties of direct trust, indirect trust and trust community detection. Used algorithms are walk-based community detection algorithm, ACL algorithm. But this ACL algorithm has trouble in the further fine-grained identification of legitimate users.

## Problem Definition

It allows unknown users to chat or text and sharing of files specially word document.

There is no additional feature like Rating in OSN's like face book ,twitter, Renren.

Miss Sushma Torvi, Assistant Professor, Dept of CSE, BLDEA's Vachana Pitamaha Dr. P.G. Halakatti College of Engineering and Technology, Vijayapur, India

Miss Pallavi koli, Miss Sumayya Islampur, Miss Sabiha Khanam M Bagawan, Miss Savita Golabavi UG Scholar, Dept of CSE, BLDEA's Vachana Pitamaha Dr. P.G Halakatti College of Engineering and Technology, Vijayapur, India.

III. SYSTEM ARCHITECTURE

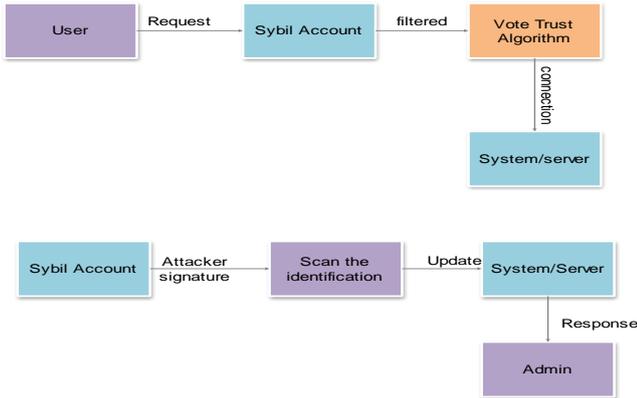


Fig.3.1:Working of votetrust system

As per the Fig.3.1, user send the request to the server where server will check the sybil account and process to vote trust based on the user request .It establish the connection with user to user finally for the social communication.

Flow Chart

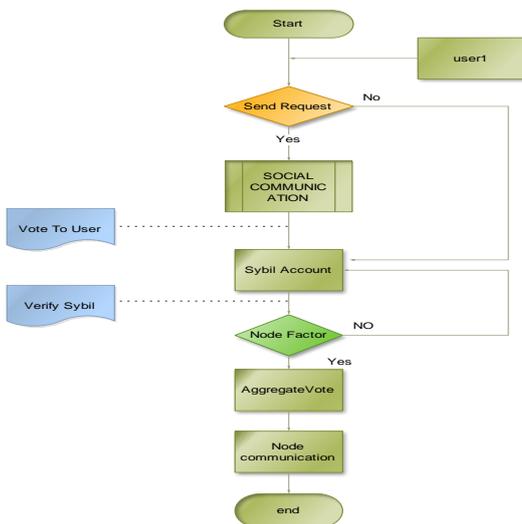


Fig 3.2: Flow chart of votetrust system

IV. MODULE DESCRIPTION

Registration: User should get register with cloud server .User enter the name, email id and mobile number .once registration is done they will get auto generated id and password in the mail and mobile.

Login: User and Admin will get login with this module .

User :will get login on the server by entering user ID and password.

User: is responsible to do upload, download, make a friend ,share a request for vote trust between trusted friend ,analysis of the vote and decide to make new friend on this .

User can requesting to make a friend using Nodes, Node Selection Source and Destination, Social Communication and File Sharing.

Admin: Login to the Server, Node Management, View the Active User and report the Sybil Attacks.

Social Communication: Here user can make a friend and send request to other also . User can have chat with other user also. User can share the data in the group to the other user who is friend. This module help to make communication based on

the node and concept . Here we assume all the user is in ideal node and have good communication to each other . Our software does not give permission to disturb someone privacy in the group, In that scenario the user becomes Sybil in the network and can't operate any operation.

V. EXPERIMENTAL RESULTS

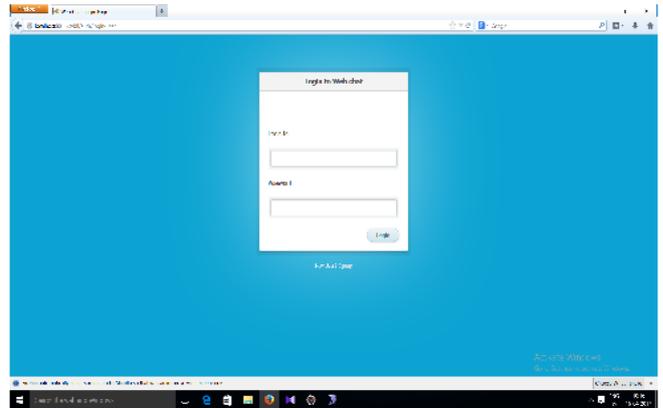


Fig.6.1: login page

In the login user has to enter the username and password to validate his identity.

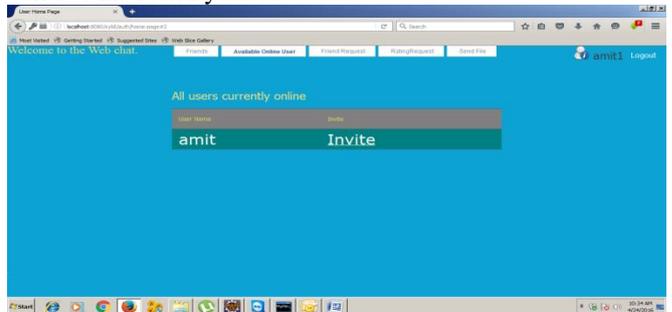


Fig.6.2: Available online users

To check current available online users to invite and communicate.

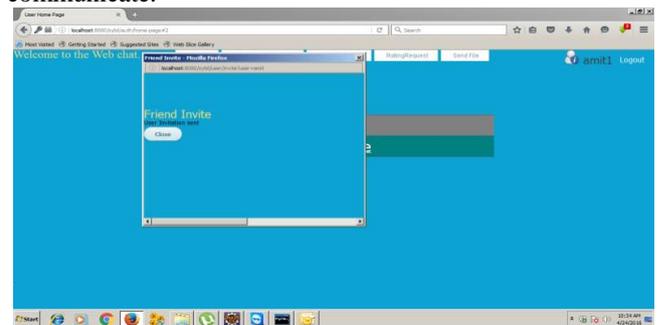


Fig.6.3: Send invite to online user

Sending request to known online users.

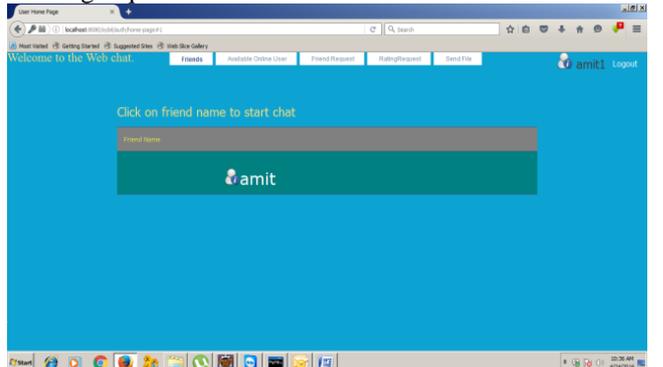


Fig.6.4: Accept the friend and view in friend.

In this page user accepts the request of other users.

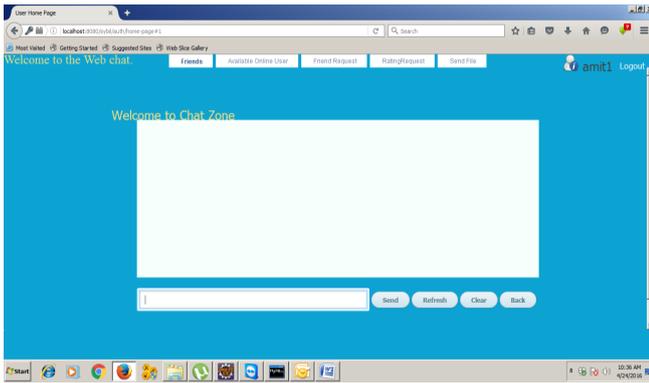


Fig.6.5: Web chat Application

Here users chat with their friends.

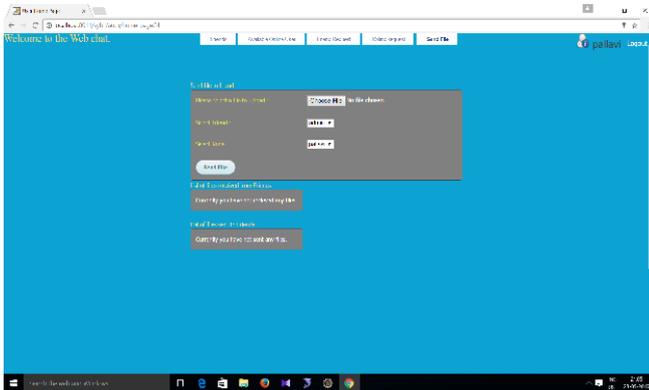


Fig 6.6:File transfer.

Here users share their word or any document to other users.

## VI. CONCLUSION

We provide the security guarantees of VoteTrust, demonstrating that we limit the number of requests Sybils can send to real users. Our evaluation over real network shows that VoteTrust is able to detect real Sybils with high precision, and significantly outperforms traditional ranking systems. Although we also use some standard techniques (e.g., a Page Rank-style algorithm to propagate scores), we make three notable contributions: First, we introduce a new graph model for Sybil defense, which nicely combine link structure and user feedback. Second, we propose new technique, including global vote aggregation and local community expansion, to exploit the negative links.

## REFERENCES

- [1] H.Gao , et.al , proposed in the work, “Detecting and characterizing social spam campaigns” in *Proc. of IMC*, 2010.
- [2]Jing Jiang, et.al, in the work,“Detecting and Validating Sybil Groups in the Wild 2012”
- [3]Amit A. Amleshwaram , et.al, in the work, “CATS: Characterizing Automation of Twitter Spammers” 2013
- [4]Guangchi Liu, et.al, in the work, “Uncovering the Mystery of Trust in An Online Social Network” 2015
- [5]H.Yu,M.Kaminsky,P.B.Gibbons,and Flaxman,“Sybilguard: defending against sybil attacks via social networks,” in *Proc. Of SIGCOMM*, 2006.
- [6]H.Yu,P.B.Gibbons,M. Kaminsky, and F. Xiao, “Sybillimit: A near-optimal social network defense against sybil attacks,” in *Proc. of IEEE S&P*, 2008.
- [7]W.Weï,F.Xu, C. C.Tan, andQ, Li, “Sybildefender: Defend against sybil attacks in large social networks,” in *Proc. of INFOCOM*, 2012.

- [8]G.Danezis and P. Mittal, “Sybilinifer: Detecting sybil nodes using social networks,” in *Proc of NDSS*, 2009.
- [9] N.Tran, B. Min, J. Li, and L. Subramanian, “Sybil-resilient online content voting,” in *Proc. of NSDI*, 2009.
- [10] B. Viswanath,A. Post, K. P. Gummadi, and A. Mislove, “An analysis of social network-based sybil defenses,” in *Proc. of SIGCOMM*, 2010.
- [11] 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 *Proc. of INFOCOM*, 2013.
- [12] J. Jiang, C. Wilson, X. Wang, P. Huang, W. Sha, Y. Dai, and B. Y. Zhao, “Understanding latent interactions in online social networks,” in *Proc. of IMC*, 2010