Defending Social Networks Against Sybil Attacks

Abstract—In the online social networks, the large number of real users can be affected by the various Sybil account. Sybil accounts means the person having the fake account and giving the unwanted friend requests and messages to the real users. In the existing system, the Sybils were only isolated by using the page ranking algorithm. The fake accounts were detected but they were again activated. The best approach to permanently deactivate the Sybil accounts is by using E-VoteTrust algorithm. E-VoteTrust Algorithm is a robust against manipulations of the graph. The goal of E-VoteTrust-based votes assignment is to assign low vote capacity to Sybils and deactivate those fake accounts.

Keywords: E-VoteTrust, Sybil Guard

I. INTRODUCTION

In the social networks, Sybil attacks can be identified[1]. These Sybils may have multiple fake accounts. They increase their power to attack the real users. The unwanted messages from the Sybils can be stored in the spam and malware can affect the large number of users like in renren[2], facebook[3], twitter[4].

To defend against Sybils, prior Sybil defenses [5]–[9] leverage the positive trust relationships among users, and rely on the key assumption that Sybils can befriend only few real accounts [10]. In this fake account users can be identified by based on the ‘accept or reject vote’ based. The users send a reject vote means it will be considered as a negative vote that is -1. Based on the highest vote the fake users can be ranked and detected. After detection that fake users again send an unwanted messages to the real users.

To deactivate the sybils, proposed system uses the E-Vote trust algorithm. By using this algorithm, the threshold value can be set to deactivate the sybils.

Figure 1: Sybil attack in Social networks

II. LITERATURE SURVEY

J. R. Douceur[1] finds the Sybil in the social network but didn’t take measures to detect them. Z.Yang, C.Wilson, X.Wang, T.Gao[2] describes the sybil accounts created to unfairly increase the power or resources of a single malicious user. They have not been able to perform large-scale measurements to detect them or measure their activities.

H.Gao, J.Hu, C.Wilson, Z.Li, Y.Chen[3] detects the social spam fake account users in the network.

H.Yu, P.B.Gibbons, M.Kaminsky, F.Xiao[4], Decentralized distributed system such as peer-to-peer systems are particularly vulnerable to Sybil attack, where a malicious user pretends to have multiple identities (called Sybil nodes), Without a trusted central authority.

J.Jiang, C.Wilson, X.Wang, P.Huang[5] separates Sybils and non-Sybils either more restrictive or permissive, thereby trading false positives for false negatives. While the designers of the schemes offer rough guidelines. Q.Cao, M.Sirivianos, X.Yang, and T.Pregueiro[6] describes the system should mostly rank nodes that are Sybils lower than non-Sybils (low false positive), while limiting the number of non-Sybils ranked below Sybils (low false negatives). It should be robust under various attack strategies. A very high portion of the nodes at the bottom of the ranked list should be fake. The portion of fakes can decrease as we go up the list.

G.Stringhini, M.Egele, C.Krugel, and G.Vigna[7] “the ratio of friends to followers of A is lower than trace. In Twitter terminology, friends are those accounts that A follows. This threshold is useful to discard those accounts that do not have many followers. Since Twitter Account Markets sell followers in batches of 3,000 such accounts are unlikely to be market customers.” J. Xue, Z. Yang, X. Yang, X. Wang [8] describes by using VoteTrust, a Sybil detection system that further leverages user interactions of initiating and accepting links. VoteTrust uses the techniques of trust-based vote assignment and global vote aggregation to evaluate the probability that the user is a Sybil.

S. Ghosh, B. Viswanath, and F. K. et al [9] mentioned that Twitter has emerged as a popular platform for discovering real-time information on the Web, such as news stories and people's reaction to them. Like the Web, Twitter has become a target for link farming, where users, especially spammers, try to acquire large numbers of follower links in the social network.

J. Jiang, C. Wilson, X. Wang [10] mentioned that recent studies have shown that a majority of user interactions on OSNs are latent interactions, passive actions such as profile browsing that cannot be observed by traditional measurement techniques. In this paper, we seek a deeper understanding of both visible and latent user interactions in OSNs.

III. PROPOSED SYSTEM

E-VoteTrust Algorithm is robust against manipulations of the graph. The goal of trust-based votes assignment is to assign low vote capacity to Sybils. Our algorithm could leverage the implicit information of negative links, and thus is able to accurately identify the Sybil community.

A. Module Description
i. Topology Construction

Topology construction is designed to construct one topology with available nodes. Register all nodes which are
involved to transfer the data to some other nodes. Depends upon total nodes, topology will be constructed. Topology construction module allows you to construct node path. If already exits, it will not allow to construct that same path. All nodes are mentioned in topology construction. User can't modify node information after construction.

ii. Node Entry

Node entry module describes node authentication. To activate node who are all involved in topology, node should be login into that topology. It does not allow unauthorized node entry. Many nodes can enter into that mentioned topology. Each node can send the messages to their destination after login.

iii. Message Transmission

Each node (source node) can send the data to some other node (destination) which one connected with that source node. While sending message, the source node should mention the header information. Source node can send the data to destination. Destination will receive that message.

iv. Sybil Guard

Sybil Guard is maintained in this project to detect the attacker. Sybil Guard is called as centralized server. Sybil Guard does not allow hackers to send the wrong data. It compares node information and header information. If matches, it assumes like normal user sending the message to destination. Otherwise Sybil Guard will not allow the hackers to send message.

v. Detection of Sybil Account

We designed and implemented Topology, a system that detects fake accounts sending out unwanted friend requests. Topology augments the social graph with social rejections, and seeks the minimum aggregate acceptance rate cut. With this formulation, our system is able to uncover friend spammers in a easy way. Our evaluation results show that topology is effective in a broad range of scenarios, attack strategies, and computationally practical.

B. System Architecture

![System Architecture Diagram]

In the above System Architecture, the user enters into the social network as usual and enters query on browser and it searches in server database. And it analysis the user searching query and generate feedback session by using the Classified Average Precision (CAP). Then it finds related data based on pseudo document over the restructured search document. In Sybil Guard the user’s status of acceptance and rejection gets stored in the V-Count database. If the vote is to Reject it assigns -1 or if its Accept then it assigns means +1. Finally with the majority of rejection the Sybil has been detected and then deactivated by the administrator.

C. Algorithm Description

Our algorithm attempts to choose C0 in a self-adjusting manner. Let m be the size of C0 in the current iteration (initially, C0 = V0s). The algorithm first expands the community C from C0. Then, the algorithm starts a new iteration, doubles the size of C0 by including top 2m nodes with the highest bad score, and re-expands the community C. This process is repeated until the expanded Sybil communities are similar at the end of two consecutive iterations, implying the whole Sybil community is enclosed. Then the algorithm outputs C as the detected Sybil community.

CONCLUSION AND FUTURE ENHANCEMENT

E-VoteTrust, is a system that leverages user interactions of initiating and accepting links to defend against Sybil attacks. We provide the security guarantees of E-VoteTrust, demonstrating that we limit the number of requests Sybils can send to real users. Our evaluation over real network shows that E-VoteTrust is able to detect real Sybils with high precision and significantly outperforms traditional ranking systems. Finally, working closely with Renren security team, we have deployed E-VoteTrust system at Renren, showing that E-VoteTrust can accurately detect real, large-scale Sybil collusion existing in the network.

In the future, Renren would execute VoteTrust periodically to detect newly created Sybils. After the detection threshold has been bootstrapped, Renren can use an adaptive feedback scheme. The setup algorithm takes as input a security parameter and outputs the public key and the master key. Note that the master key is kept secret at PKG. Verify the attribute of user, who does the function of data. Secure the attribute of data hold user.

References
