

Product Review Recommendation System with Sybil Detection

Abinaya V.¹, ShebaKeziaMalarchelvi P. D.²

PG Scholar, Department of CSE, J.J. College of Engineering and Technology, Tiruchirappalli, India¹

Professor and Head, Department of CSE, J.J. College of Engineering and Technology, Tiruchirappalli, India²

Abstract— Unethical users increasingly find Online Social Networking (OSN) platforms as lucrative targets for malicious activities, such as sending spam and spreading malware. In particular, attackers leverage the open nature of OSNs and send unwanted friend requests known as friend spam to legitimate users and it has been proven to be the most evasive malicious activity. This might happen due to sybils. A Sybil attack happens when an insecure computer is seized by use of force to claim multiple identities which are used to send friend spams. One of the many systems that are being affected by sybils is a product review system wherein sybils might provide reviews for a product. These reviews may not be trustworthy and hence should not be taken into account for ranking a product. Hence in this project, a product review recommendation system that filters out the reviews provided by sybils based on friend request rejection rate and review rejection rate has been proposed to suggest trustworthy reviews for potential buyers of a product.

Index Terms— Friend Request Rejection Rate (FRR), Review Rejection Rate (RRR), Spam, Sybil Attack, Sybils

I. INTRODUCTION

The Sybil attack in computer security is an attack wherein a reputation system is undermined by forging identities in peer-to-peer networks. Malicious user creates multiple fake identities known as sybils to increase their power and influence within the target community (JilongXue *et al.*, [8]). Sybils forward spam and malware to the real users and access the private information. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder. It does not provide Secure communication. Sybils can establish connection with real users by sending a large amount of requests. Online social networks (OSNs) currently face a significant challenge by the existence and continuous creation of fake user accounts (Sybils), which can undermine the quality of social network service by introducing spam and manipulating online rating (JilongXue *et al.*, [8]). Sybils does not include fake accounts generated by users for benign purposes, such as preserving privacy and anonymity, acting on behalf of young children, separating work and personal identities, etc. These “benign Sybils” act just like normal accounts, and do not fall under our definition of malicious Sybils (Zhi Yang *et al.*, [9]).

The system has one or more honest human beings as honest users and has one or more malicious human beings as malicious users. Honest nodes obey the protocol. The identities

created by malicious users are called as sybil identities/nodes. All sybil nodes are controlled by an adversary. The adversary may eavesdrop on any messages sent in the protocol (Haifeng Yu *et al.*, [3]). The edges connecting the honest region (i.e., the region containing all the honest nodes) and the sybil region (i.e., the region containing all the sybil identities created by malicious users) are called attack edges (Haifeng Yu *et al.*, [10]). The edges between the Sybils are known as Sybil edges (Zhi Yang *et al.*, [9]).

B. Viswanath *et al.*, [6] used a metric called conductance for determining how closely a subset of nodes within a network are connected among themselves relative to the rest of the network. G.Danezis *et al.*, [2] used Bayesian inference technique to determine the probability of any node in the system being marked as non-Sybil. N. Tran *et al.*, [5] used adaptive vote flow aggregation technique to limit the number of bogus votes cast by adversaries to no more than the number of attack edges in the trust network (with high probability). Haifeng Yu *et al.*, [10] described the Random walk is performed by each node. It marks a suspect node as non-Sybil if the random walk from the trusted node and the suspect intersect otherwise marks as a Sybil.

In section II we present an elaborate survey of various Sybil defense techniques found in the literature. In sections III and IV we present the proposed system and in section V we present the conclusion.

II. RELATED WORK

A. Zhi Yang *et al.*, [9]

Zhi Yang *et al.*, described their efforts to detect, characterize and understand Sybil account activity in the Renren online social network (OSN). They use the ground truth provided by Renren Inc. to build measurement based Sybil account detectors, and deployed them on Renren to detect over 100,000 Sybil accounts. They conducted a brief survey of three software tools. They are Renren Marketing Assistant V1.0, Renren Super Node Collector V1.0, Renren Almighty Assistant V5.8. The purpose of these tools is to automate the process of creating Renren accounts, forming edges between the Sybils and other users, and posting content en-mass. The tools select targets for friending by performing snowball sampling to locate popular users. They applied a Support Vector Machine (SVM) classifier to the ground truth dataset of 1000 normal users and 1000 Sybils. The results showed that the classifier is very accurate. Adaptive threshold based sybil detector

monitors all accounts using a combination of friend request frequency, outgoing request acceptance rates, and clustering coefficient.

B. Haifeng Yu et al., [3]

SybilGuard protocol uses a key insight on social networks to bound the number of sybil nodes accepted but it can allow a large number of sybil nodes to be accepted. Haifeng Yu et al., presented the novel SybilLimit protocol that uses the same insight as SybilGuard, but offers dramatically improved and near-optimal guarantees. They used the protocol because: 1) it limits the number of sybil nodes accepted and 2) it is near-optimal and thus pushes the approach to the limit. SybilLimit has two component protocols: a secure random route protocol and a verification protocol. Secure Random Route Protocol focused on all the suspects in SybilLimit and performed random routes. A suspect S starts a random route and propagates along the route its public key K_S together with a counter initialized to 1. Let "A→B" be the last edge traversed by S's random route and it is called the tail of the random route. Node B would see the counter having a value of W (length of random route) and thus record K_S under the name of that tail. The verification protocol, requires that S know A's and B's public keys and IP addresses. After the secure random route protocol stabilizes, a verifier V can invoke the verification protocol to determine whether to accept a suspect S. S must satisfy both the intersection condition and the balance condition to be accepted.

C. W. Wei et al., [7]

SybilDefender is a sybil defense mechanism that consists of three components: sybil identification algorithm to locate the sybil nodes, a sybil community detection algorithm to detect the sybil community surrounding a sybil node, and two proposals for limiting the number of attack edges in online social networks. The sybil identification algorithm takes the social graph $G(V, E)$, a known honest node h , and a suspect node u as inputs, and outputs whether u is Sybil or not. A random walk on a graph is defined by the sequence of moves of a particle between nodes of G . The intuition of sybil identification algorithm is that, as there is a small cut between the honest region and the sybil region, the random walks starting from a sybil node tend to get "trapped" into the sybil region. They defined the number of times one node being travelled by a set of random walks as the frequency of that node. The sybil community detection algorithm uses the social graph $G(V, E)$ and a known sybil node s as inputs, and outputs the sybil community around s . The algorithm relies on performing partial random walks originating from s . Each partial random walk behaves the same as the standard random walks except that it does not traverse the same node more than once. Therefore, when a partial random walk arrives at a node with all the neighbors traversed by itself, this partial random walk is "dead" and cannot proceed.

D. Qiang Cao et al., [4]

SybilFence is a system that is based on the observation that even well-maintained fake accounts unavoidably receive a significant number of user negative feedback, such as the rejections to their friend requests. Their key idea is to discount the social edges on users that have received negative feedback, thereby limiting the effect of Sybils' social edges. Most of them bound the undetectable Sybils to the number of attack edges i.e. $O(\log n)$ Sybils per attack

edge. They observed that the attack edges from Sybils are usually accompanied by the negative feedback from cautious real users, who are resistant to abusive communication. A negative feedback can be refusing to accept a friend request or to report on receiving unwanted communication. Promiscuous users have high tolerance of abusive activities and unwanted communication, while cautious users are more resistant to fake accounts. A real user will not experience negative feedback if she never sends out unwanted communication. SybilFence comprises of two major modules: 1) a negative feedback combiner, which incorporates the negative feedback graph into the social graph, and generates a defense graph with discounted social edges on the users that have received negative feedbacks and 2) an adopted social graph-based defense strategy that detects Sybils on the defense graph with improved accuracy.

E. Bimal Viswanath et al., [1]

Social network-based Sybil defense schemes are divided into two categories: Sybil detection and Sybil tolerance. These two categories of systems leverage global properties of the underlying social graph, but they rely on different inferences and provide different guarantees: Sybil detection schemes are application-independent and depends only on the graph structure to identify Sybil identities, while Sybil tolerance schemes rely on application-specific information and use the graph structure and transaction history to bound the leverage an attacker can gain from using multiple identities. The goal of Sybil detection is to label identities in the system as either Sybil or non-Sybil. They could make it impossible for all detected Sybil identities to interact with other identities in the system. All Sybil defense strategies can be modeled as, first, inducing a ranking on all the identities from the perspective of the true identity and second applying a cut-off on the ranking that is determined by scheme-specific parameters. Nodes ranked before the cut-off are marked as non-Sybil and identities ranked after the cut-off are marked as Sybil. Nodes that are tightly connected to the true identity are more likely to be ranked higher. Tolerance assumes that users perform pairwise deals (e.g., sending a message, purchasing an item, casting a vote). They achieve a defense against Sybils by allocating credits to the network links, and then allowing actions only if paths with sufficient credit exist between the source and destination of an action.

III. PROPOSED SYSTEM

The proposed system is used to defend a product review system against sybils. In the product review system the users give reviews about different products. Two types of users are available in Social network namely sybil user and real user. To identify whether the user is a sybil or not, it checks the friend request rejection rate and the review rejection rate. This focuses on the friend invitation behavior, and detects Sybils that get more rejections than acceptances from real users and updates the user status as 1 for normal user and -1 for sybil user. After identification of Sybil users the reviews provided by them are listed as Sybil user reviews which may be skipped by a user who reads the reviews.

IV. PROPOSED SYSTEM ARCHITECTURE

A. Admin module

In this module admin provides authentication code for each community e.g. Reporter, IT, Manager. This Authentication code is used to validate the user. Admin can add new communities, view all communities, view the list of users, normal and sybil

community. He can view all user's products and details. Admin updates the user status as 1 for normal user and -1 for sybil user.

B. User Module

In this module users create their own profile, login, view their profile, search other users, send friend request to them, add new products, give description for those products, view friend list, view request list, search products, recommend/ not recommend those products to other users by casting votes, view the reviews for the products (trusted and sybil user reviews) and likes/dislikes other user's reviews.

C. User Validation

User U_i logs-in, selects a product to order and reads the reviews of the valid users. Users are validated by checking whether the particular user has provided the review for the product or not. If the user has provided review for that product then checks whether the user is a sybil or not. If the user has not provided the review for that product then checks the next user. If the user is a sybil then his review is rejected otherwise it is read.

D. Sybil Detection

For all the users other than the user i who has currently logged, this module checks whether the user has provided review for the particular product or not. If the user has provided review for that product then checks whether the user is a sybil or not. To identify whether the user is a sybil or not, it checks the Friend Request Rejection Rate (FRR) and the Review Rejection Rate (RRR).

$$FRR \text{ rate} = \left(\frac{TFR - AFR}{TFR} \right) \times 100 \quad (1)$$

where TFR is the Total number of Friend Requests sent and AFR is the number of Accepted Friend Requests .

$$RRR = \left(\frac{TPR - PRL}{TPR} \right) \times 100 \quad (2)$$

where TPR is the Total Number of Product Reviews given by a user and PRL is the Number of Product Reviews Liked by other users.

Using (1) and (2), we calculated the Friend Request Rejection Rate (FRR) and the Review Rejection Rate (RRR) respectively. If the friend request rejection rate is greater than or equal to 50% then he is a sybil user and reject his review otherwise check the review rejection rate. If the review rejection rate is greater than or equal to 70% then reject the review otherwise read the review as depicted in the fig 1. This focuses on the friend invitation behavior, and detects Sybils that get more rejections than acceptances from real users. If the user has not provided the review for that product then checks the next user.

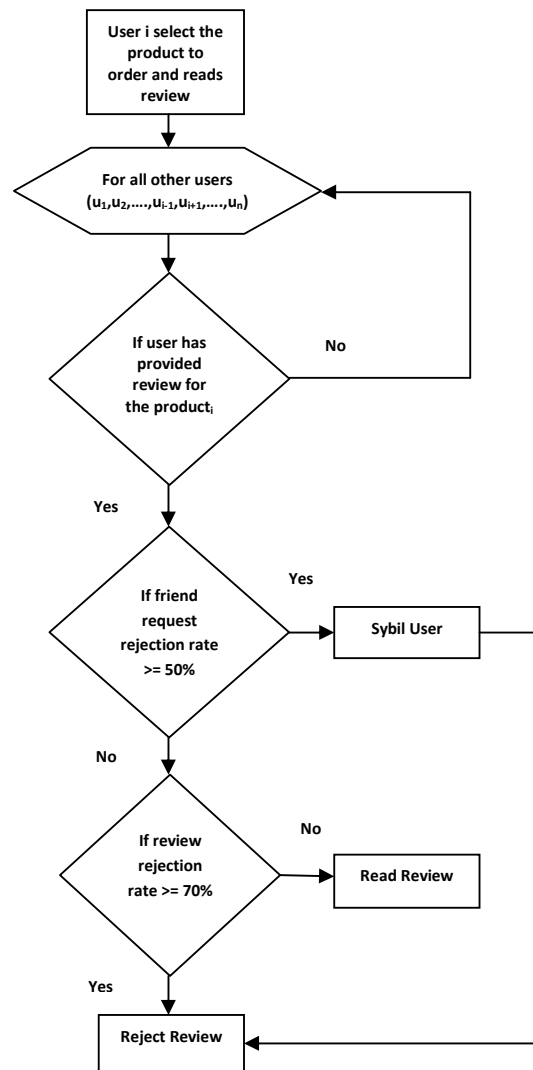


Fig. 1. System Architecture

E. Product Module

In this module, the user adds new products and gives description about it. User can search the products and recommend/ not recommend it to other users by voting. Both sybil and non-sybil users can give reviews about the products. Admin can view all user's products, view both sybil and non-sybil user's voting for the product. The product rating calculation is based on the user's voting. Both sybil and non-sybil users can search the products and their details. Both users can recommend the product to other users.

F. Voting Validation

This module is used to validate the user's voting based on the user type. The user type may be Sybil user or Real user. The voting for product consists of two ranking namely Trust rank and Sybil rank. It also detects the Sybil community.

V. EXPERIMENTAL ANALYSIS



Fig 2.Home Page



Fig 6. Product Review



Fig 3.Add New Product

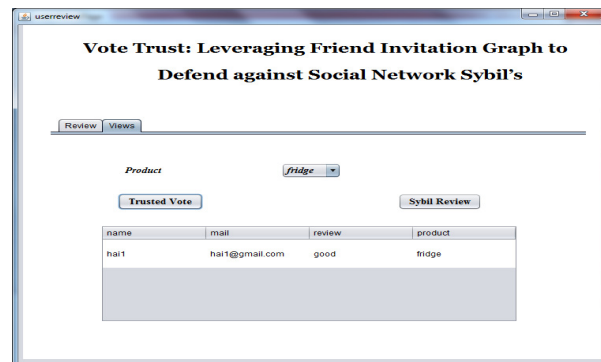


Fig 7.View Reviews



Fig 4.View Request List

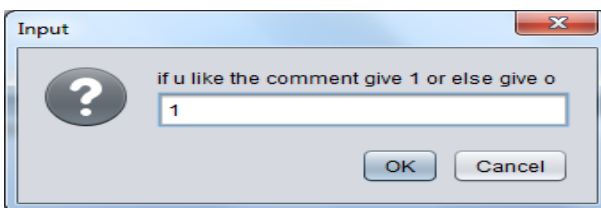
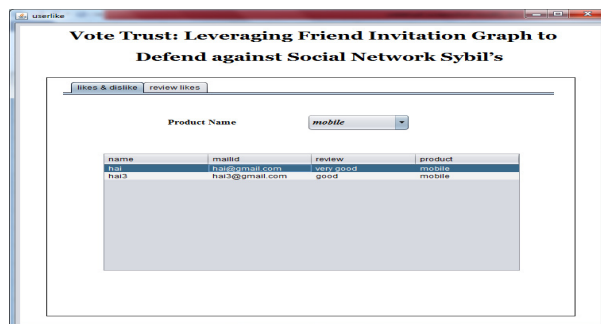


Fig 8.User Likes and Dislikes for Product Reviews

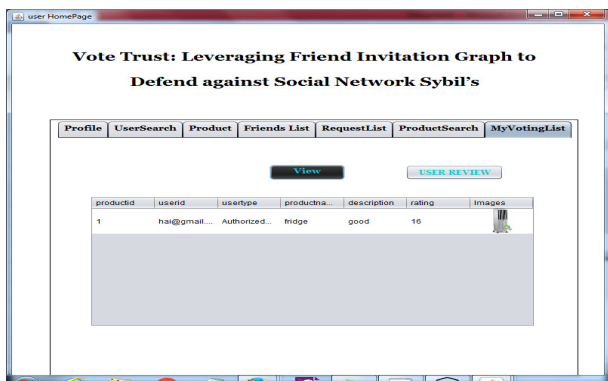


Fig 5.View Voting List

VI. CONCLUSION

OSNs are vulnerable to Sybil attacks. With this attack, a malicious user creates multiple fake identities, known as Sybils, to unfairly increase their potential and influence within a target community. Sybils forward spam and malware on the social networks such as Renren, Facebook and Twitter. There is a distinct difference between Sybils and real users in terms of the acceptance

rate, i.e., the fragment of outgoing friend requests accepted by real users. Sybils might cause problems in many application areas of OSNs. One particular application is a product review system. In this case, sybils might act as real users and can cast positive votes to enhance the opinion about a product. Hence in this project a system has been proposed to defend a product review system against sybils. The proposed system focuses on the friend invitation performance, and detects Sybils that get more rejections than acceptances from real users. It detects and prevents sybil attack. It identifies the sybil community. In this proposed system, assumptions have been made about the friend requests and rejections without actually integrating OSNs. In future this product review system can be integrated with OSNs.

REFERENCES

- [1] Bimal Viswanath, Mainack Mondal, Allen Clement, Peter Druschel, Krishna P. Gummadi, Alan Mislove and Ansley Post, "Exploring the design space of social network-based Sybil defenses", in Proceedings of the Fourth International IEEE Conference on Communication Systems and Networks (COMSNETS), 2012.
- [2] Danezis. G and Mittal. P, "Sybilinfer: Detecting sybil nodes using social networks", in Proceedings of the Network and Distributed System Security Symposium (NDSS), 2009.
- [3] Haifeng Yu, Phillip B. Gibbons, Michael Kaminsky and Feng Xiao, "SybilLimit: A Near-Optimal Social Network Defense Against Sybil Attacks", ACM Transactions on Networking (ToN), 2010.
- [4] Qiang Cao and Xiaowei Yang, "SybilFence: Improving Social-Graph-Based Sybil Defenses with User Negative Feedback", in Proceedings of the IEEE conference on Social and Information Networks, 2013.
- [5] Tran. N, Min. B, Li. J, and Subramanian. L, "Sybil-resilient online content voting", in Proceedings of the 6th USENIX Symposium on Networked systems design and implementation, 2009.
- [6] Viswanath. B, Post. A, Gummadi. K. P and Mislove. A, "An analysis of social network-based sybil defenses", in Proceedings of Association for Computing Machinery's Special Interest Group on Data Communications Conference, 2010.
- [7] Wei. W, Xu. F, Tan. C. C and Li. Q, "Sybildefender: Defend against sybil attacks in large social networks", in Proceedings of the IEEE Conference on Computer Communications, 2013.
- [8] Xue. J, Yang. Z, Yang. X, Wang. X, Chen. L, and Dai. Y, "Votetrust: Leveraging friend invitation graph to defend against social network sybils", in Proceedings of the INFOCOM, 2013.
- [9] Yang. Z, Wilson. C, Wang. X, Gao. T, Zhao. B. Y and Dai. Y, "Uncovering social network sybils in the wild", in Proceedings of the ACM SIGCOMM conference on Internet measurement conference (ICM), 2011.
- [10] Yu. H, Kaminsky. M, Gibbons. P. B, and Flaxman. A, "Sybilguard: defending against sybil attacks via social networks," in Proceedings of the SIGCOMM conference on Applications, technologies, architectures, and protocols for computer communications, 2008.