ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.8

Sybil Detection via Geo-location Analysis in Online Social Network

Mayuri A. Shirsath[1], Prof. Rahul M. Chinchore[2]
ME Student[1], Assistant Professor[2]
Department of Computer Science and Engineering
GHRIEM, Jalgaon, MS, India

Abstract:
Distributed systems without trusted identities are particularly Week able to sybil attacks, where an again stars creates multiple Untruth full identities to compromise the running of the system. Here we dedicate two approaches first, votetrust a sybil defense mechanism that leverages the network topologies to defend against sybil attacks in social networks. votetrust outperforms the state of the art by one to two orders of magnitude in both accuracy and running time. Votetrust can effectively identify the sybil nodes and detect the sybil community around a sybil node, even when the number of sybil nodes introduced by each attack edge is close to the theoretically detectable lower bound. Second, we introduce a min radius based definition to capture users mobility patterns, which is used to measure the radius of a user's activity region.

Keywords: social networks, social network-based Sybil defense, Location-Based Feature, detection.

I. INTRODUCTION

Social networking sites allow users to create personal profiles, share images and to connect with a large network of friends and often with a lot of strangers. In order to reach a user on OSNs like Renren and Facebook, the attacker must first befriend that user. This is because, by default, social communications such as creating posts are only allowed between friends. The Sybils cannot be monetized without first establishing social connections to real users. This motivates us to exploit the friend request behavior to detect Sybils. The current social graph-based Sybil defenses assume that the key difficulty of Sybils is to befriend many real users [1]. However, our results show that Sybils can easily overcome this difficulty by sending a large amount friend requests. Their actual difficulty is to require real users to befriend them first or to accept them with a high probability. In the past few years, online social networks have gained great popularity and are among the most frequently visited sites on the Web. The large sizes of these networks require that any scheme aiming to defend against sybil attacks in online social networks should be efficient and scalable. Some previous schemes can achieve good performance on a very small network sample but their algorithms are computationally intensive and cannot scale to networks with millions of nodes .Based on the above rationale, We present vote trust, a centralized sybil defense mechanism. It consists of a sybil identification algorithm to identify the sybil nodes, a sybil community detection algorithm to detect the sybil community surrounding a sybil node, and two approaches to limiting the number of attack edges in online social networks [2].

II. LITERATURE REVIEW

In this section, we propose a survey about how to detect and prevent the Sybil attacks and the mechanisms.

H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman proposed that SybilGuard, a novel protocol for limiting the corruptive influences of Sybil attacks. This protocol is based on the "social network" among user identities, where an edge between two identities indicates a human established trust relationship. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately-small "cut" in the graph between the sybil nodes and the honest nodes. SybilGuard exploits this property to bound the number of identities a malicious user can create. Sybil Guard guarantees that an honest node accepts, and also is accepted by, most other honest nodes with high probability. Thus, an honest node can successfully obtain service from, and provide service to, most other honest nodes. SybilGuard also guarantees that with high probability, an honest node only accepts a bounded number of Sybil nodes. SybilGuard leverages the existing human-established trust relationships among users to bound both the number and size of Sybil groups.[3]

B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove proposed that Sybil defense to detect local communities (i.e., clusters of nodes more tightly knit than the rest of the graph) around a trusted node. Malicious attackers can create multiple identities and influence the working of systems that rely upon open membership. 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 Sybil[4]

W.Wei, F. Xu, C. C. Tan, and Q. Li proposed that Sybil defender. It is a Sybil defense mechanism that leverages the network topologies to defend against Sybil attacks in social networks. Based on performing limited number of random walks within the social graphs, SybilDefender is efficient and scalable to large social networks. Sybil Defender consists of two components: a Sybil node identification algorithm, a Sybil group around that Sybil node detection algorithm.[5]

G. Danezis and P. Mittal, describe Sybilinfer proposed that It is a centralized approach used to mitigate Sybil attacks in social networks. The process starts from a known trusted node, taken as reference, and then Sybil probability is assigned to each node using Bayesian Inference. In other words, it assigns the rank to each node which is nothing but the degree of Sybil certainty. Sybil infer is suitable for networks which holds only up to 30K nodes and it is not scalable to larger networks. But it is only scalable to smaller networks.[6]

GuangchiLiu, Qing Yang, Honggang Wang, Xiaodong Linz and Mike P proposed that Assessment of Multi-Hop Interpersonal Trust in Social Networks.it is Three-valued subjective logic is proposed to compute the interpersonal trust between any two persons who have not had interactions before. 3VSL introduces posteriori uncertainty space to store the evidences distorted from certain spaces as trust propagates, and priori uncertainty space to control the evidence size as trusts combine. They also discover the differences between distorting opinions and original opinions, i.e. original opinions are so unique that they can be reused in trust computation while distorting opinions are not.[7]

H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, Sybillimit In this research work they have proposed a novel SybilLimit protocol that takes advantages of the same insight as Sybil Guard but offers dramatically improved and near-optimal guarantees. Finally, based on three large-scale real- world social networks, we provide the first evidence that real-world social networks are in fact fast mixing. But it cannot detect more than one Sybil node at a time.[8]

III. PROPOSED APPROACH

We now describe the implementation of our proposed work, which is the stage of the project when the theoretical design is turned out into a working system.

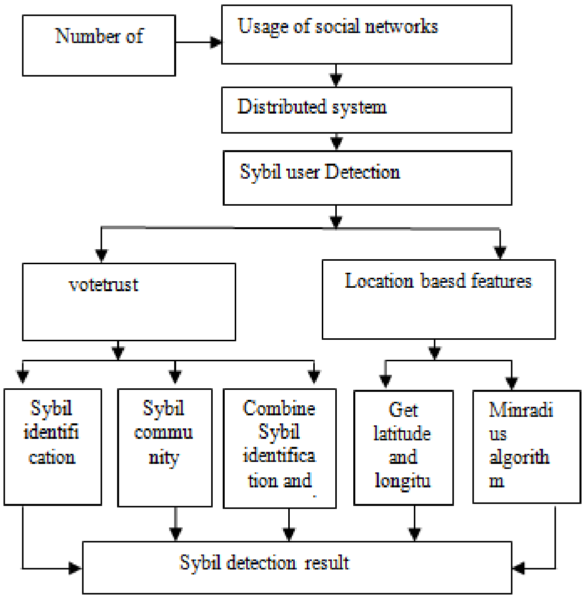


Figure.1.System Architecture

- **User Module:**

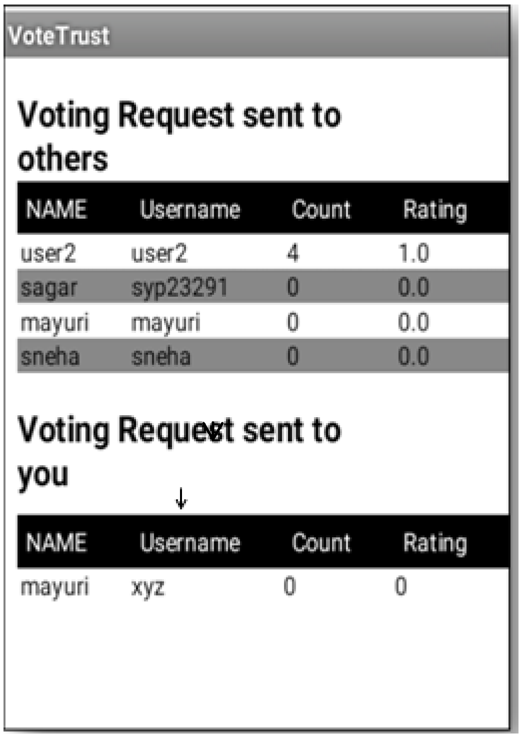
In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first.

- **Sybil Community Detection Algorithm:**

After one sybil node is identified, our sybil community detection algorithm can be used to detect the sybil community surrounding it. The sybil community detection algorithm takes the social graph G(V,E) and a known sybil node s as inputs, and outputs the sybil community around s. The sybil node s can be identified by our sybil identification algorithm. We define a sybil community as a subgraph of G consisting of only sybil nodes, and there is no small cut in this sub graph. The reason why we make this definition is that if a small cut does divide the sybil region into two parts S1 and S2, and the known sybil node s is in S1, then, from the point of view of s, the honest region and S2 are similar, since there is already a small cut between S1 and the honest region and also a small cut between S1 and S2. When there is a small cut in the sybil region, our algorithm can detect the sybil community s belongs to. Our 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.

- **Votetrust :**

SybilDefender consists of three components: a sybil identification algorithm, a sybil community detection algorithm, and two supporting approaches to limiting the number of attack edges. The three components can be used in conjunction to best mitigate sybil attacks. The task of the sybil identification algorithm presented to determine whether a suspect node is sybil or not. Then we show how to efficiently detect the sybil community around a sybil node with our sybil community detection algorithm presented.



VoteTrust

Voting Request sent to others

NAME	Username	Count	Rating
user2	user2	4	1.0
sagar	syp23291	0	0.0
mayuri	mayuri	0	0.0
sneha	sneha	0	0.0

Voting Request sent to you

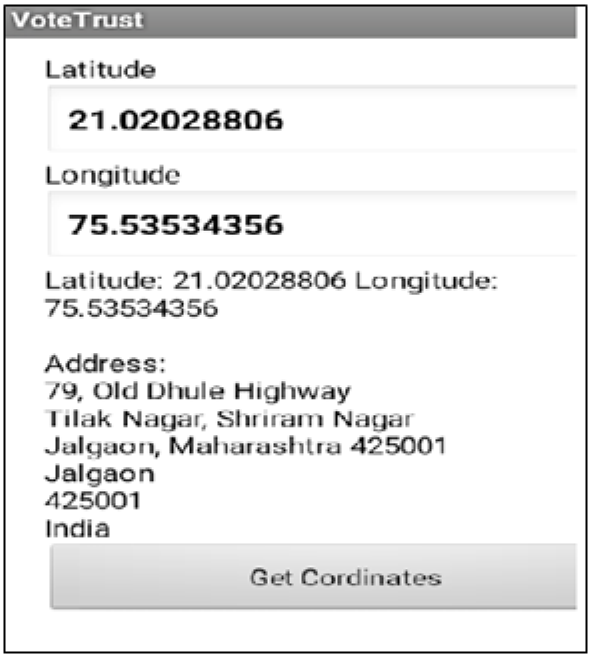
NAME	Username	Count	Rating
mayuri	xyz	0	0

Figure.1. users voting.

VoteTrust uses two key techniques, trust-based vote assignment and global vote aggregating, to properly assign the vote capacity and to compute the global acceptance rate. Then, it can identify the Sybil for which the majority of votes are negative.

- **Location baesd features:**

It gives the accurate information of current location of user. It shows the latitude and longitude of the current location of user. Here GPS tracker gives the current address of user And to capture a user's mobility pattern, we define the concept of smallest radius of a user's daily minimum covering circles minRadius, which is used to measure the radius of a user's activity region. The main idea of this algorithm is to determine two points that are on the border of the minimum covering circle. At the beginning, two points are chosen as endpoints of the diameter to construct a circle. Then we add other points to this circle one by one. If any point is not in this circle, this point must be on the border of a new circle which covers the point itself.


VoteTrust

Latitude

21.02028806

Longitude

75.53534356

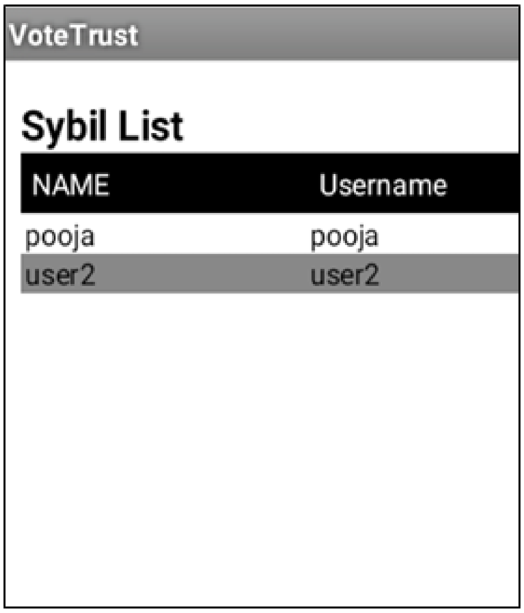
Latitude: 21.02028806 Longitude:
75.53534356

Address:
79, Old Dhule Highway
Tilak Nagar, Shriram Nagar
Jalgaon, Maharashtra 425001
Jalgaon
425001
India

Figure.3.Location of user

- **Detection:**

It gives bad score propagation is to find nodes that are more likely to be colluders. Low vote propagation indicates a high likelihood of being Sybil.


VoteTrust

Sybil List

NAME	Username
pooja	pooja
user2	user2

Figure.4. Sybil user list.

IV. EVALUATION AND ANALYSIS

Evaluation of attack detection is done by using NSL KDD dataset. Normal Profile is built by using NSL KDD Training dataset. Test profile is generated by using NSL KDD Test dataset. The Euclidian Distance is calculated for both Normal and Test Profiles. Threshold range is generated by using '$\mu + \sigma *\alpha$' and '$\mu - \sigma *\alpha$' for normal Distribution, the value of 'α' ranges from 1 to 3. Detection rate and False positive rate is evaluated for the different values of 'α'.

Performance Analysis*:*

- **Detection Rate:** The detection rate is defined the number of intrusion instances detected by the system (True Positive) divided by the total number of intrusion instances present in the test set.
- **False Alarm Rate:** Defined as the number of 'normal' patterns classified as attacks (False Positive) divided by the total number of 'normal' patterns.

Alert Type*:*

- **True Positive:** : Attack - Alert
- **False Positive:** : No attack - Alert
- **False Negative:** : Attack - No Alert
- **True Negative:** : No attack - No Alert

Terms:

- **True Positive:** A legitimate attack which triggers IDS to produce an alarm.
- **False Positive:** An event signalling IDS to produce an alarm when no attack has taken place.
- **False Negative:** When no alarm is raised when an attack has taken place.
- **True Negative:** An event when no attack has taken place and no detection is made.

V. CONCLUSION

The proposed system would be efficient and scalable to large social networks, a scheme that leverages network topologies to defend against Sybil attacks in large social networks. We have provide the security guarantees of VoteTrust, demonstrating that we limit the number of requests Sybils can send to real users VoteTrust can accurately detect real, large-scale Sybil collusion existing in the network. This work shows that three notable contributions: First, introduce a new graph model for Sybil defense, which nicely combine link structure and user feedback. Second, they propose new techniques, including global vote aggregation and local community expansion, to exploit the negative links. Our evaluation over real network shows that location-based features are important factors to detect sybil users**.**

VI. REFERENCES

[1].J. Xue, Z. Yang, X. Yang, X. Wang, L. Chen, and Y. Dai, "Votetrust: Leveraging friend invitation graph to defend against social network sybil," in Proc. of INFOCOM, 2013.

[2].D. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-resilient online content voting," in Proc. USENIX Netw. Syst. Design Implement. (NSDI), 2009, pp. 15–2

[3]. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman., “SybilGuard: Defending against Sybil attacks via social networks,” in SIGCOMM, 2006.

[4].B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, “An analysis of social network-based Sybil defenses,” in SIGCOMM, 2010.

[5].W.Wei, F. Xu, C. C. Tan, and Q. Li, “Sybildefender: Defend against sybil attacks in large social networks,” in Proc. of INFOCOM, 2012.

[6].G. Danezis and P. Mittal, “Sybilinfer: Detecting Sybil nodes using social networks,” in Proc of NDSS, 2009.

[7].GuangchiLiu, Qing Yang, Honggang Wang, Xiaodong Linz and Mike P in “Assessment of Multi-Hop Interpersonal Trust in Social Networks by Three- Valued Subjective Logic”.

[8].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.

[9].J. R. Douceur, “The Sybil attack,” in Proc. of IPTPS, March 2002.

[10].Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai, “Uncovering social network sybils in the wild,” in Proc. of IMC,2011.

[11].Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, “Aiding the detection of fake accounts in large scale social online services,” in nsdi, 2012.