ISSN: 2321-7782 (Online)
Volume 4, Issue 2, February 2016
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Comparative Study on Techniques of Sybil Attack Detection

Ubale Tushar G[1]
Computer Science
G.H Raisoni College of Engg & Management
Ahmednagar - India

Pathan Mohsin M[2]
Computer Science
G.H Raisoni College of Engg & Management
Ahmednagar - India

Sose Sachin L[3]
Computer Science
G.H Raisoni College of Engg & Management
Ahmednagar - India

Asst. Prof. Shendre Priti B[1]
Dept of Computer Engineering
G.H Raisoni College of Engg & Management
Ahmednagar - India

Abstract: ***The Sybil's are fake user. Sybil attack is a type of security threat when nodes in network claim multiple identities. In this Paper we review the different methods of detecting the Sybil attack in network. We make comparison of those methods and identify the relevant method to detect Sybil identity. Also a mechanism of vote trust is discussed in proposed system which gives more efficient results for the detection of Sybil's.***

Keywords: Sybil, OSN, vote trust, Sybilguard, Sybillimit, SybilDefender.

I. INTRODUCTION

OSNs have come under Sybil attacks. In Sybil attack, a malicious user creates multiple fake identities, known as Sybils, to disproportionately enlarge their power and influence within a target community. Researchers have observed Sybils forwarding spam and malware on Renren, Facebook and Twitter

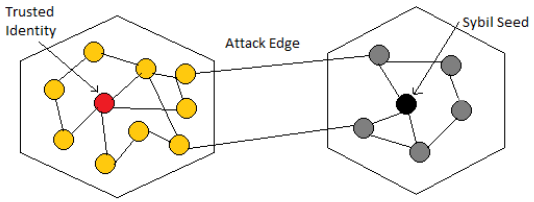

Fig. Sybil Attack

To defend against Sybil, prior Sybil defenses leverage the positive trust relationships among users, and rely on the key assumption that Sybil's can befriend only few real accounts. Unfortunately, we find that people in real OSNs still have a non-zero probability to accept friend requests of strangers, leaving room for Sybils to connect real users through sending a large amount of requests.

Therefore, we present Vote Trust that uses friend invitation interactions among users that has a directed, signed graph and utilizes Voting based Sybil detection and sybil community detection to detect sybils over the graph. A Sybil attack depends on the fact that a network of computers cannot ensure that each unknown computing node is a discrete, physical computer, as described by Microsoft researcher John Douceur. Sybil attacks have appeared in many scenarios, with wide implications for security, safety and trust. For example, an internet poll can be rigged using multiple IP addresses to submit a large number of votes. Some companies have also used Sybil attacks to gain better ratings on Google Page Rank. Reputation systems like eBay's have also been victims of this type of attack.

II. EXISTING TECHNIQUES

Sybil Guard: It exploits social interactions to bound the number of identities of a malicious user can create. SybilGuard's security really depends on the number of attack edges in the system, connecting honest and dishonest users. [3]. Sybil Limit: It is a protocol that leverages the same insight as SybilGuard but offers dramatically improved and near-optimal guarantees. [4] Sybil Defender: It is a Sybil defense mechanism that leverages the network topologies to defend against Sybil attacks in social networks. [5][6] Sybil Infer: It uses a probabilistic model of honest social networks, and an inference engine that returns potential regions of dishonest nodes. [6]

III. LITERATURE SURVEY

1] Sybil Guard [3]: Proposed a sybil guard protocol for limiting the corruptive influences of sybil attacks. And that protocol is based on the "social network" among user identities, where an link between two identities that indicates a human-established trust relationship. But Sybil guard is that it cannot detect more than one Sybil node at a time. In Sybilguard method can reject some trusted nodes and (mistakenly) consider two or more distinct trusted nodes as equivalent.

2] Uncovering Social Network Sybils in the Wild [2]: In this paper the main two approach for Sybil detection on OSNs. First, the ground-truth data about the behavior of Sybils in the wild to create a measurement based, real-time Sybil detector with calculations of low false positive and negative rates. And second contribution is a first-of-its-kind characterization of Sybil graph topology on a major OSN. With this technique No studies have demonstrated their efficacy at detecting Sybils in the wild.

3] Sybillimit [4]: In this research work they have proposed a novel SybilLimit protocol that takes advantages of the same insight as SybilGuard 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.

4] Sybil Defender [5]: 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] Sybil Infer [6]: 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] Combating Web Spam with TrustRank [7]: Possible ways to implement the seed present results of experiments run on the World Wide Web indexed by AltaVista and evaluate the performance of our techniques. TrustRank can be used either separately to filter the index, or in combination with PageRank and other metrics to rank search results.

7] Exploiting Mobile Social Behaviors for Sybil Detection [8]: In this research work they have proposed a social-based mobile Sybil detection scheme to detect four levels of Sybil attackers with different attacking capabilities. They have investigated mobile user's pseudonym changing behaviors compared with that performed by Sybil attackers, and utilized contact statistics as the criteria of pseudonym changing for mobile Sybil detection. The security analysis demonstrates that the SMSD can resist four levels of Sybil attackers, while the extensive trace based simulation can validate the detection accuracy of the SMSD [1].

8] Sybil Attacks and Their Defenses in the Internet of Things [10]: Here they have provided a survey of Sybil attacks and their defense schemes in IoT. Specifically, they have defined three types of Sybil attacks in the distributed IoT and presented some Sybil defense schemes with the comparison. The differential characteristics, including social structures and behaviors, between Sybil attackers and normal users could facilitate the Sybil defense. In addition, MSD can leverage mobile network features, wireless channel characteristics, and cryptography to resist Sybil attackers. They have some disadvantages research issues such as Sybil defence in MSNs, tradeoffs between privacy and learning in Sybil defence, and cooperative Sybil defence.

9] Combating Friend Spam Using Social Rejections [11]: Here they contribute to fight against fake accounts that act as friend spammers in Facebook-like symmetric OSNs, driven by the observation that even well-maintained fake accounts certainly have their friend requests rejected by the legitimate users end. They propose Rejecto, a system that detects accounts that send out unwanted friend requests. Rejecto 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 manipulation-resistant way. We evaluate Rejecto through extensive simulations that are driven with real-world OSN samples. We also evaluate our parallel implementation on an EC2 cluster evaluation results show that Rejecto is effective in broad range of scenarios.

10] Assessment of Multi-Hop Interpersonal Trust in Social Networks [9]: 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. They validate 3VSL both in theory and real world evaluation. The results indicate that 3VSL is sound and can be applied in computing trust with high accuracy. Bayesian analysis will be integrated to make 3VSL is not able to from multiple sources.

IV. PROPOSED SYSTEM

After the Survey of above literature regarding Sybil attack and its solution in online social network the proposed solution coming from the comparison of this above method which is discussed in below section.

We now describe the design of our proposed work, which considers the fake user detection as a vote aggregation problem. In this application a link of the friend invitation graph means that one node casts a certain number of votes for the other users. The vote value is determined by the sign of link. For each node user, VoteTrust guarantees that votes are mainly collected from real users by pruning the collusion votes among fake users. Further the system identifies the fake user for which the majority of votes are negative.

In VoteTrust Mechanism, We conclude that a node B release a (positive or negative) vote on a node A. if B either accepts or rejects the request from A. VoteTrust first uses a PageRankstyle algorithm to exact assign the number of votes that one can release on another node. This process assigns few vote capacity for individual Sybils and thus saved them from significantly guaranteed each other through collusion.

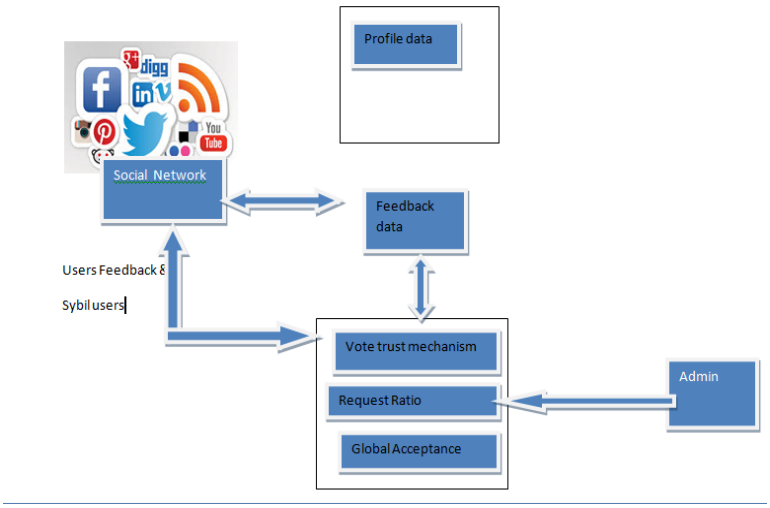

Fig. Mechanism

After that VoteTust compute a global acceptance rate(i.e. real user probability). For each node through aggregating the vote over the online social network. In this aggregation penalizes vote from suspected node. Due to more negative vote from trusted user,sybil user would get low global acceptance rate and thus sybil user identified out.

V. COMPARATIVE STUDY

SybilGuard, SybilLimit, SybilInfer, and SumUp are all algorithms for performing decentralized detection of Sybil nodes on social graphs. At their core, all of these algorithms are based on two assumptions of Sybil and normal user behavior but in the proposed method used methodologies of vote aggregation and propogation.

VI. CONCLUSION

Sybil attack is most crucial in distributed decentralized systems like social networks. We have also discussed some techniques to defend against Sybil attack. In order to prevent the Sybil attacks first we provided the mechanisms used to detect the Sybil, second the approaches used to identify the bending from Sybil nodes. In this paper we review the different way to identify the fake/sybil/false accounts in online social networks and proposed solution for the detection.

References

1. Zhi Yang, JilongXue, Xiaoyong Yang, Xiao Wang, and Yafei Dai,"VoteTrust: Leveraging Friend Invitation Graph to Defend against Social Network Sybil, 2015.
2. 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.
3. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against Sybil attacks via social networks," in Proc. of SIGCOMM, 2006.
4. 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.
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. Z. Gyongyi, H. Garcia-molina, and J. Pedersen, "Combating web spam with trustrank," in VLDB. Morgan Kaufmann, 2004, pp.
8. Kuan Zhang, Xiaohui Liang, Rongxing Lu, Kan Yang IN "Exploiting Mobile Social Behaviors for Sybil Detection" in the 2015 IEEE conference :
9. 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"
10. Kuan Zhang, Xiaohui Liang, in "Sybil Attacks and Their Defenses in the Internet of Things" in IEEE internat of things journal ,vol.1,no 5,octomber 2014
11. Qiang Cao Michael Sirivianos, Xiaowei Yang Kamesh Munagala in "Combating Friend Spam Using Social Rejections".

AUTHOR(S) PROFILE

Ubale Tushar G, Studying in VIII semester of Bachelor of Engineering in Computer Engineering from G.H Raisoni college of Engg & Management Chas, Ahmednagar (Savitribai Phule Pune University). And Area of interest is Network Security.

Pathan Mohsin M, Studying in VIII semester of Bachelor of Engineering in Computer Engineering from G.H Raisoni college of Engg & Management Chas, Ahmednagar (Savitribai Phule Pune University). And Area of interest is Network Security.

Sose Sachin L, Studying in VIII semester of Bachelor of Engineering in Computer Engineering from G.H Raisoni college of Engg & Management Chas, Ahmednagar (Savitribai Phule Pune University). And Area of interest is Network Security.

Asst. Prof. Priti B. Shendre, received the M.Tech degree in Computer Science and Engineering and B.E degrees in Information Technology from RTMNU Nagpur Univerrsity in 2014 and 2011, respectively. Currently working as an asst. Prof. In from G.H Raisoni college of Engineering & Management Chas, Ahmednagar in Computer Engineering Department. And Area of interest is Image Processing, Network Security.