 ISSN: 2321-8169
47 – 51

Defense Mechanism Techniques against Sybil Attack

Miss. Ankita S. Koleshwar
Research Scholar
SGB Amravati University,
Amravati, India
ankita.koleshwar12@gmail.com

Mrs. S. S. Sherekar
Dept. of Computer Science & Engg,
SGB Amravati University,
Amravati, India
ss_sherekar@rediffmail.com

Dr. V. M. Thakare
Dept. of Computer Science & Engg,
SGB Amravati University,
Amravati, India
vilthakare@yahoo.co.in

Abstract *:* In today's globe, use of social networking sites are increased. Thus many users are trying to form multiple bogus identities to negotiate the running of the system. Sybil means multiple bogus identities in social network. Sybil attacks are well known and powerful attack against online social network. In this paper, the various types of Sybil attacks are given which are based on behavior of attacker. This paper gives the different types of current Sybil defense protocols like SybilGuard, SybilLimit, SybilDefender, SybilInfer, Symon etc to defend against Sybil attack.

Keywords: *SybilGuard, SybilLimit, SybilDefender, SybilShield, SybilInfer, Symon.*

*****

I. INTRODUCTION

In an Online Social Network all users are not honest users. A malicious user creates fake identities and suppresses the opinions of honest users[1]. In the presence of Sybil attacks, many systems may generate wrong reports and user might receive spam and lose their privacy. According to the report in 2012, a significant nos. of user accounts are confirmed as fake accounts or Sybil accounts in Online Social Network, totally 76 million (7.2\%) in facebook, and 20 million fake accounts created in twitter per week. Many recent research efforts have been focused on studying Sybil attack and how to detect and defend them. Practical examples of Sybil attack. such as (i) Rig Internet polling by using multiple IP addresses to submit votes.(ii) Increase Google Page-Rank rating of a page. (iii)Reputation systems (iv) Bugmenot.com.

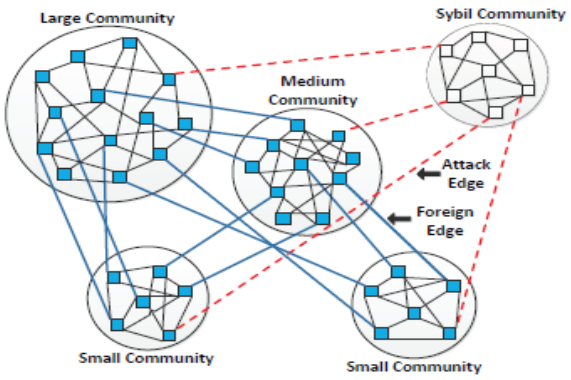
Sybil attack proves to be a threat to the recommendation system reducing its robustness. If an attacker maliciously creates many identities, it can easily change popularity of the system. Due to Sybil attack the honesty of the following domains are affected.

- Mobile networks
- Wireless sensor networks
- Online social networks

In this paper, such Sybil attack detection mechanisms are discussed in which SybilGuard, SybilLimit, SybilInfer, SybilDefender etc are included.

II. BACKGROUND

Most social network based Sybil detection schemes work on the random walk approach and assume that most of the Sybil identities generally establish connections only with Sybil identities and tend to remain in their own community. A recent study in online social network Renren, states that the number of social connections established between Sybil users and honest users is growing exponentially and an experiment states that in a social network Sybil users generally won't establish connections with other Sybil users[2]. In real time social networks, considering the pace at which Sybil identities are multiplying, social network based approaches alone wouldn't be sufficient to detect the Sybil attacks which led to many novel anti-Sybil approaches based on user's behavior.



In behavior based anti-Sybil schemes, the users browsing and clicking habits are considered to separate Sybil users from normal users. The general activities performed by a user in online social networks are uploading pictures, viewing other's photos and profiles, sending messages, sharing content, playing games, posting blogs and commenting on the blogs. Unlike normal users, Sybil users activities are quite narrow such as befriending (Send friend requests and establish connections), sending messages and sharing content with others which are considered to be the main sources to spread spam and malware in social networks.

Considering the click transitions as a Markov chain, a random process which changes from one state to another, and assuming each click pattern as a different state, it can be observed that normal user's behavior is unpredictable and changes from one state to another randomly whereas Sybil users 10 participate only in specific activities repeatedly. The Support Vector Machine approach (SVM) has been proposed to monitor specific features such as clicks in particular time period, number of clicks in a session, time interval between two clicks and other features which yielded high results to detect Sybil activity. Another study proposes three models namely click sequence model, time-based model and hybrid model, which combines similar click patterns for analyzing the users behavior. Based on some standard similarity measurements, a graph is constructed which is used to detect Sybil users. Wang et al, proposes a Sybil detection scheme based on crowd-sourcing and Social Turing test. Turing test is the ability of a machine to think intelligently similar to a human being. Even though, if an attacker has a wide range of tactics, she cannot pass the turing test which increases the detection efficiency. In addition, crowd sourcing provides a platform for users to share their opinions, ideas and provide ratings to improve the Sybil detection accuracy.

III. CLASSIFICATION OF SYBIL ATTACK

Sybil attack was first addressed in peer to peer system. The attacker subverts the reputation system of peer to peer network by creating a large number of misrepresents identities[3].

The classification of different types of Sybil attacks is discussed below.

1) *Insider vs Outsider* : Both attackers, insider or outsider, both directly determines the ability of the attacker, and the rigidness of introducing a Sybil attack. Distributed systems are more vulnerable to inside attackers.
2) *Selfish vs Malicious* : Selfish attackers manipulate the false data just for their own benefit, while malicious attackers attempt to subvert a system.
3) *Directed vs Indirected Communications* : The attacker can directly communicate with an honest node by using one of her Sybil Identities, or she can use only her real identity to communicate with others, and route the Sybil data via this real identity. For the attackers, direct communication with honest nodes directly influences the success of attacking. The attackers with more directed communications are harder to detect.
4) *Simultaneously vs Gradually Obtained Sybil Identities* : The attacker can obtain all of her Sybil identities simultaneously, or she can gradually generate them one by one.
5) *Busy vs Idle* : All Sybil identities can participate in a distributed system simultaneously, or only some of them can work, while others are in an idle state.
6) *Discarded vs Retained* : For an attacker, how to manage the old Sybil identities is important. After finding a Sybil node, one can further identify the others by monitoring the claimed communication between a suspect node and the detected Sybil node. Since the attacker is not aware of whether the old identities have been detected yet, once in a while, she has to determine whether or not to discard them.

IV. SYBIL ATTACK DOMAIN

If a single malicious node is able to convince its neighbors by presenting multiple identities, it will have control over the substantial portion of the network and can adversely affect the functioning of this network[3]. Once a Sybil attack has been launched in the system, it also opens the doors for different types of other attacks. The applications which are affected by Sybil Attack are given as follows :

a) *Routing* : Sybil attacks can also impact the functioning of certain routing protocols in MANETs such as geographic based routing protocols and multi-path routing protocols. In geographic routings, the nodes exchange their location information with their neighbors, to route the packets in an efficient manner.
b) *Records Aggregation* : A single Sybil attacker with multiple fake identities can participate in the aggregation, a number of times and can alter the result of the data aggregation.
c) *Voting* : A Sybil attacker node is also capable of altering the result of a voting scheme. For example, in a vote based intrusion detection system, a malicious node with multiple Sybil nodes can expel a legitimate node from the network by voting against this node. Also, to win the trust of the legitimate nodes in the network, a Sybil attacker can take advantage of its multiple Sybil nodes that will vote in its favor.
d) *Fair Resource Allocation* : Fair resource allocation scheme is also affected by the Sybil attack. For example some network resources may be allocated on a per node basis; in that case a malicious node can have a larger share of any resource by presenting multiple identities.

IV. DEFENSE MECHANISM AGAINST SYBIL ATTACK

Social network based Sybil defense mechanisms are mostly decentralized solution, which means these design operate without any centralized authority. All social networks based Sybil defenses mechanism has two common assumptions: Algorithmic property (called the fast mixing property) and trust. Social network based Sybil defenses are based on the fast mixing property of social graphs. Fast mixing property of social graph implies that the nodes in the social graphs are well trapped and there is no Sparse-cut in the graph.

1) *SybilGuard* : Introduced SybilGuard. SybilGuard is a novel protocol for detecting Sybil attack in social network[4]. SybilGuard is based on the "social network" among user identities, where an edge between two identities point out a human-established trust relationship.

Malicious users can create many fake identities but few trust relationships. SybilGuard relies on these two properties.

 ISSN: 2321-8169
47 – 51

a) The honest region of the network is fast mixing. Fast mixing property of the social graph implies honest region does not contain a sparse cut.

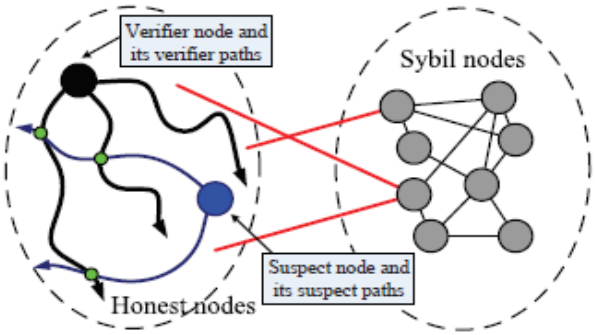


Fig : Honest path verification

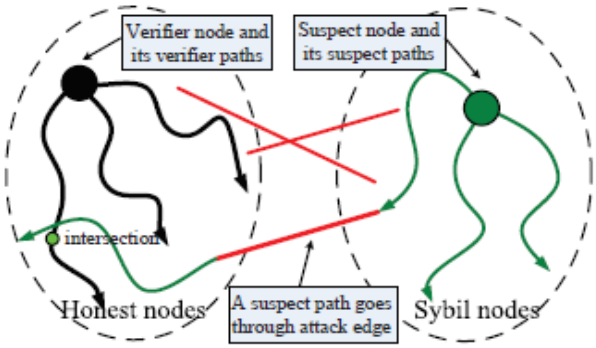


Fig : Sybil path verification

Above fig shows the social graph with Sybil node and honest node. If there is a relationship between the honest node and Sybil node then it is considered as an Attack edges.

b) Malicious user may create many nodes but relatively few attack edges. SybilGuard ensures two measures for detecting Sybil attack. First measure is the number and size of the Sybil groups is properly bounded for 99.8\% of the honest users. Second measure is the honest node can accept, and be accepted by 99.8\% of all other honest nodes. SybilGuard define two terms: l.Trusted node 2.Trustted path. SybilGuard assumes there is a trusted node in a social graph.

2) *SybilLimit* : SybilLimit is also using similar principle of SybilGuard. SybilLimit is a completely decentralized protocol[5]. The advanced version of SybilGuard is SybilLimit that reduce the Sybil attack value to 0 (log n). SybilGuard using the single long random walk for detecting Sybil node but SybilLimit using several shorter random walks for detecting the Sybil attack.

3) *SybilDefender* : Sybil defender is one of the famous anti-Sybil detection schemes which use community detection approach. It also uses random walkers like SybilGuard and SybilLimit but uses minimum number of random walks when compared to them[6]. The algorithm is divided in two parts (i) To find a Sybil node, (ii) To find the region surrounding the Sybil node which is assumed to be the Sybil community. The assumption is built on the fact that the numbers of attack edges are limited, i.e. the number of Sybil identities are negligible when compared to honest identities, and also the honest region is fast mixing, i.e. nodes in the honest region converge very fast when compared to Sybil region.

To detect a Sybil node we start from a known honest node and find the k-hop neighbors which are considered as honest nodes. These k-hop neighbors are considered to be honest, based on the assumption that honest region is fast mixing. These nodes serve as the boundary for the honest region. From each of these honest nodes, a large number of random walks with varying lengths are performed and the frequency distribution of nodes is observed. Frequency is defined as the number of times a random walk traverses through a node. From the suspect node also, with varying length of random walks the frequency distributions of nodes is observed. If both the distributions are same, the node is considered to be honest, otherwise it is called a Sybil node.

4) *SybilShield* : Social network based anti-Sybil schemes came into prominence due to the limitations posed by central trust authority and resource testing schemes. It uses the trust relationships in social networks to minimize the influences of Sybil attack. Sybil guard is the first approach which used social network architecture to reduce the Sybil influences[7]. Unlike previous social network based approaches, which assumes that the social network graph is divided in two regions namely honest and Sybil regions, Sybil shield assumes that there exists multiple number of large, medium and small communities in real-time social networks.

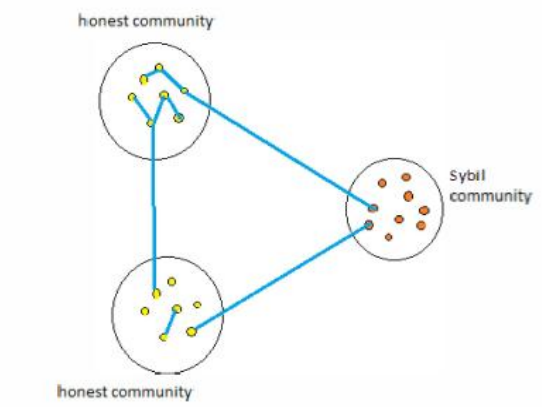


Fig : Different communities in social graph

A real-time experiment conducted on Myspace reveals that it can be divided into 19 communities, with the smallest size being 12 and the largest size of 33,887 nodes with a number of foreign edges between communities. An edge between two different communities is called a foreign edge. It also assumes that social networks are fast-mixing i.e. even though if an adversary creates large number of Sybil identities, the number of trust relationships established between an honest node and a Sybil node is limited. Therefore, foreign edges formed between honest communities are more when compared to honest and Sybil communities.

5) *SybilInfer* : Sybil Infer is a centralized approach for detecting Sybil node. In a centralized approach there is a central authority is used to detect the Sybil node[8].

The process starts from the known trusted node taken as reference and then Sybil probability is assigned using Bayesian inference. In other words, it assigns the rank to each node for detecting Sybil node. Overall time complexity of Sybil Infer is 0 (Vlogv), where V is the number of nodes in a network. Sybil Infer is only suitable for network consist of 30K nodes and it is not suitable for larger network.

6) *Symon* : Symon is a novel approaches to defend against Sybil attacks in distributed decentralized networks. It ensures honest nodes are protected from Sybil's with high probability[9]. In Symon, each and every node in the network is associated with a non-Sybil called as Symon. The non-Sybil or Symon is chosen dynamically, such that the chance of both nodes being Sybil is impossible. Each Symon is given the responsibility of monitoring the activities of the given node making it impossible for the other node to compromise the system. A Symon should make sure that a malicious node has to invest a lot of cost to create a bogus identity. In addition, in Symon approach any node in the network can verify with high probability whether a pair nodes are Sybil's or not.

7) SybilResist : Sybil-Resist, is a Random Walk-based Sybil attack defense protocol is used to detect the Sybil node in online social network[10].

There are four main parts of Sybil-Resists are given as follows :

i) Pre-processing
ii) Sybil identification
iii) Walk length estimation algorithm
iv) Sybil region detection algorithm

8) SumUp : SumUp is an anti-Sybil technique designed for a distributed voting system. Before we discuss the general idea of SumUp, we first need to understand the meaning of a credit network[3]. Credit network is a concept used in the electronic commerce field, and it is designed for building and measuring transitive trust among users. Note that, in the field of electronic commercial, trust is usually pair wise. Whenever a node (identity) trusts another node, a trust link will be established, together with certain trust value (credits). When a node gets services from others, the node can use the associated credits to pay for the services. Note that the credit network could also be used as a payment infrastructure between nodes that do not directly extend credit to each other. Two remote nodes, which do not directly trust one another, can interact with each other when there exists credit paths between them. In some systems, such interactions will cost credits from the paths.

9) *Canal* : Canal also adopts a credit network, and we can regard it as an extension of SumUp[11]. In a credit network, each interaction between nodes always requires the system to first find at least one available credit path; clearly, such a process has a high computational cost. Essentially, the procedure of searching such paths is equivalent to the maximum flow problem.

V. SUMMARY

Sr. No	Detection Mechanism	Techniques Used	Advantages	Limitations
1)	SybilGuard	Random Walk	SybilGuard offers noticeably improved	It detects only one Sybil node at a time
2)	SybilLimit	Random Walk	Improve the reliability	It works only on a fast mixing network
3)	SybilDefender	Limited Random Walk performed by node	Efficient and Scalable	Failure
4)	SybilShield	Resource Testing scheme used	SybilShield reduces false positive rate	Nos. of nodes increases the falsely detected node level also increases
5)	SybilInfer	Bayesian inference on the results of the random walks	SybilInfer is reliable than SybilGuard	Computational overhead & it is not scalable
6)	Symon	Selected dynamically	Fast mixing property	Not suitable for larger network
7)	SybilResist	Random Walk	Used to detect Sybil node in OSN	Not specified
8)	SumUp	Anti-Sybil technique	Used as a payment infrastructure	Two remote nodes do not directly trust one another
9)	Canal	Extension of SumUp	Not specified	High computational cost

VI. CONCLUSION

The main objective of Sybil defense is to take out Sybil attack by detecting Sybil nodes. This ultimate goal is not always possible due to fact that most defenses. Many recent research efforts have been focused on studying Sybil attack and how to detect and defend them. This paper focuses on the Defense Mechanism Against Sybil Attack like SybilGuard, SybilLimit, SybilInfer, SybilDefender, SybilShield etc. The existing mechanisms for detecting the Sybil attacks are not enough to comprehend with the present scenario. The limitations of existing detection mechanism are presented in this paper gives an opportunity to researchers to propose a detection mechanism addressing such issues.

REFERENCES

[1] M. Al-Qurishi, M. Al-Rakhami, A. Alamri, M. Alrubaian, S. M. M. Rahman and M. S. Hossain, "Sybil Defense Techniques in Online Social Networks: A Survey," in *IEEE Access*, vol. 5, no. , pp. 1200-1219, 2017.

[2] Wang, Feng. "Preventing Sybil Attacks in Structured P2P Networks using Social Network." *Boletín Técnico* 55.5 (2017): 424-429.

 ISSN: 2321-8169
47 – 51

[3] W. Chang and J. Wu, "A survey of Sybil attacks in networks," 2012.
[4] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, 2006. SybilGuard: Defending against Sybil Attacks via Social Networks. Proceeding ACM SIGCOMM.
[5] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, 2008. SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks. IEEE Symposium Security and Privacy.
[6] W.Wei, F. Xu, C. C. Tan, and Q. Li, ``Sybildefender: Defend against Sybil attacks in large social networks," in Proc. IEEE INFOCOM, Mar. 2012, pp. 1951 1959.
[7] L. Shi, S. Yu,W. Lou, and Y. T. Hou, ``Sybilshield: An agent-aided social network-based Sybil defense among multiple communities," in Proc. IEEE INFOCOM, Apr. 2013, pp. 1034 1042.
[8] G. Danezis and P. Mittal, ``SybilInfer: Detecting Sybil nodes using social networks," in Proc. NDSS, 2009, pp. 1 15.
[9] D. N. Tran, B. Min, J. Li, and L. Subramanian, ``Sybil-resilient online content voting," in Proc. NSDI, 2009, pp. 15 28.
[10] H.Yu, C. Shi, M. Kaminsky, P. B. Gibbons, and F. Xiao, ``Dsybil: Optimal Sybil-resistance for recommendation systems," in Proc. 30th IEEE Symp. Secur. Privacy, May 2009, pp. 283 298.
[11] B. Viswanath, M. Mondal, K. P. Gummadi, A. Mislove, and A. Post, ``Canal: Scaling social network-based Sybil tolerance schemes," in Proc. 7th ACM Eur. Conf. Comput. Syst., 2012, pp. 309 322.