Study on Techniques to Defend Against Social Network Sybils

Mrs. Rajeswari S
Sr.Assistant Professor in Information Science and Engineering, New Horizon College of Engineering Bangalore, India. E-mail: raji_sura@yahoo.com

Keerthi Priya C
Information Science and Engineering, New Horizon College of Engineering, Bangalore

Nikitha P
Information Science and Engineering, New Horizon College of Engineering, Bangalore

ABSTRACT: *Unscrupulous users increasingly find Online Social Networking (OSN) platforms as lucrative targets for malicious activities, such as sending spam and spreading malware. The profitability of such activities and the fact that a large portion of the OSN communication takes place over social links (e.g., Facebook) that are symmetric in nature, motivate attackers to connect to real users. In particular, attackers take advantage of the open nature of OSNs and send to legitimate users unwanted friend requests, also known as friend spam.These friend spams have proven to be among the most evasive malicious activities.*

KEYWORDS: spam, online social network, Sybil, peer to peer system, attack edges.

I. INTRODUCTION

A Sybil attack [1] can infuse many forged identities (called Sybils) to subvert a target system. Because of the severe damage that Sybil attacks cause to a wide range of networking applications, there has been a proliferation of Sybil defense schemes. The profitability of such activities and the fact that a large portion of the OSN communication [2] takes place over social links (e.g., Facebook [3] and Twitter [4]) that are symmetric in nature motivate attackers to connect to real users.

OSN providers build their core functionalities on social graph as shown in Fig.1, that often assume that a social graph solely consists of links which represents the social trust of user pairs, the consequences of falsely accepted requests by unsuspected users are severe. Particularly, the false OSN links resulting from friend spam can compromise the accuracy of social ad targeting and search, and the privacy of shared content by users.

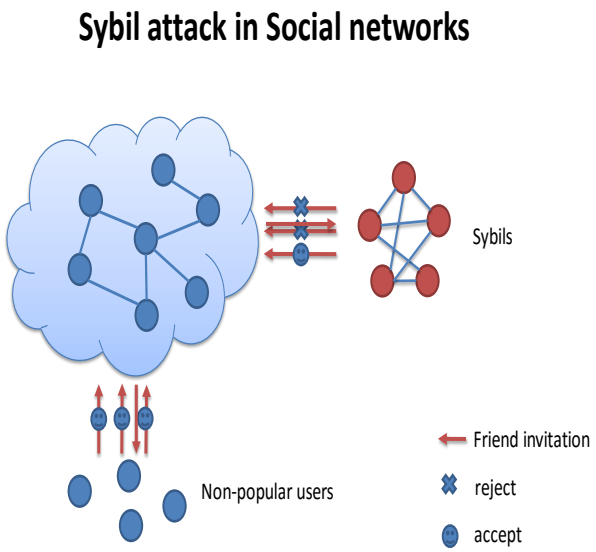


Fig.1. Sybil attacks in social network

The main barrier faced by OSN is the urgent requirement of effective Sybil defense solutions. However, under different contexts it is unclear how effective these OSN-based solutions are. For example, all current approaches have focused on a common, classical scenario where it is difficult for an attacker to create attack edges and link Sybils with honest users; however, recent researches have revealed that a modern scenario also becomes a commonplace for an attacker to employ simple strategies to obtain many attack edges.

II. TECHNIQUES

1. SYBILGUARD

SybilGuard [5], a novel protocol was proposed for limiting the corruptive influences of Sybil attacks. This protocol is based on the existence of a social network among user identities, where an edge between two identities indicates a human-established trust relationship. Though malicious users can create many identities they can have only a few trust relationships.

SybilGuard is a decentralized protocol that restricts the corruptive influence of Sybil attacks, including Sybil attacks launched from botnets outside the system and even some Sybil attacks exploiting IP harvesting. This design is based on a unique insight regarding social networks, where user identities are nodes in the graph and (undirected) edges are trust relations (e.g., friend relations) that are human-established. The honest region (i.e., the region containing all the honest nodes) and the Sybil region (i.e., the region containing Sybil identities created by malicious users) are connected by edges called attack edges as shown in Fig. 2. This protocol ensures that the number of attack edges is restricted by the number of trust relation pairs between malicious users and honest users, and does not depend on the number of Sybil identities.

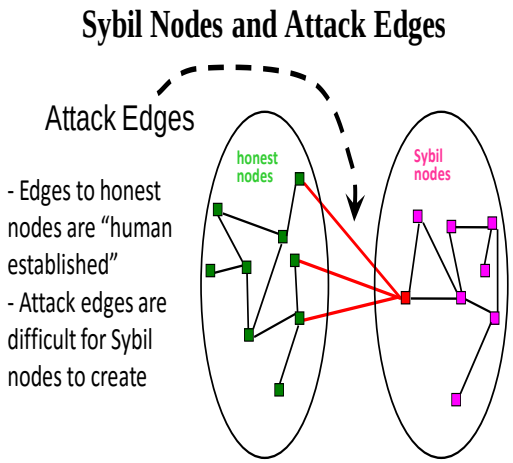


Fig. 2.Sybil Nodes and Attack Edges

SybilGuard guarantees that an honest node accepts, and also is accepted by, most other honest nodes (except a few propotion in our later simulation) with high probability as shown in Fig. 3. Thus, an honest node can successfully provide service to and obtain service from most other honest nodes. SybilGuard also guarantees that with high probability, an honest node only accepts a limited number of Sybil nodes.

If two nodes are connected by an edge, we can say that the two users are friends. Notice that here the edge indicates strong trust. An edge may exist between a Sybil node [6] and an honest node if a malicious user (Jenny) successfully fools an honest user (Ashley) into trusting her. Such an edge is called an attack edge .The authentication system in SybilGuard ensures that regardless of the number of Sybil nodes Jenny creates, Ashley will at most share an edge with one of them (as in the real social network). Thus, the number of attack edges is restricted by the number of trust relation pairs that can established between honest users and malicious users by the adversary.

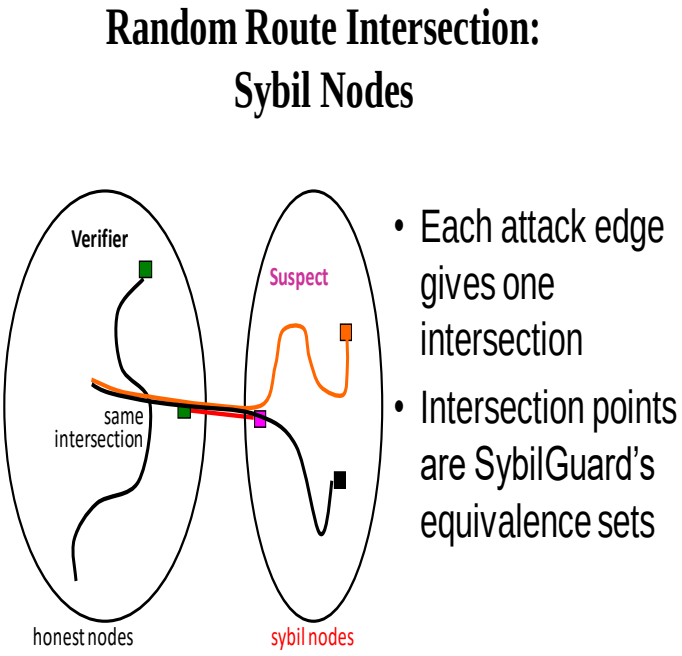


Fig. 3. Random Route Intersection

1.1.Limitations

- ♣ These techniques rely on the assumption that fakes can befriend only few real accounts. This assumption is not valid.
- ♣ Sybils could still increase their scores by befriending even more victims.
- ♣ They cannot and do not aim to control the number or size of Sybil groups.

2. SYBILINFER

SybilInfer [7] is an algorithm which can be used for labeling nodes in a social network as honest users or Sybils controlled by an adversary as shown in Fig.4. SybilInfer is secure, as it can successfully distinguish between honest and dishonest nodes and is not susceptible to manipulation by the adversary.

SybilInfer applies to settings where a peer-to-peer or distributed system is somehow based on or is aware of the social connections between users. Properties of natural social graphs are used to classify nodes are honest or Sybils.

Although this approach might not be applicable to very traditional peer-to-peer systems [8], it is more common for designers to make distributed systems aware of the social environment of their users. Linking all dishonest nodes with each other (without adding any Sybils) changes the characteristics of their social sub-graph, and can be detected under some circumstances, in SybilInfer. This approach demonstrates the practical efficacy of our approach using both synthetic scale-free topologies as well as real-world data, also propose extensions that enable our solution to be implemented in decentralized settings. SybilInfer shows significant security improvements over both Sybil-Limit and SybilGuard, the current state of the art Sybil defense mechanisms

2.1. Overview

The SybilInfer algorithm takes a social graph G as an input and a single known good node that is part of this graph. The conceptual steps as shown below are then applied to return the probability each node is honest or controlled by a Sybil attacker:

- A set of traces T are generated and stored by performing special random walks over the social graph G. These are the only retained information about the graph for the rest of the SybilInfer algorithm.
- A probabilistic model is then defined based on our assumptions that social networks are fast mixing, while the transitions to dishonest regions are slow.
- Once the probabilistic model is defined, we use the traces T and Bayes theorem to calculate set of honest nodes. As it is not possible to simply enumerate all sub-sets of nodes of the graph G, we instead sample from the distribution of honest node sets.

The key technical challenge is making use of this distribution to extract probability if each node is honest or dishonest.

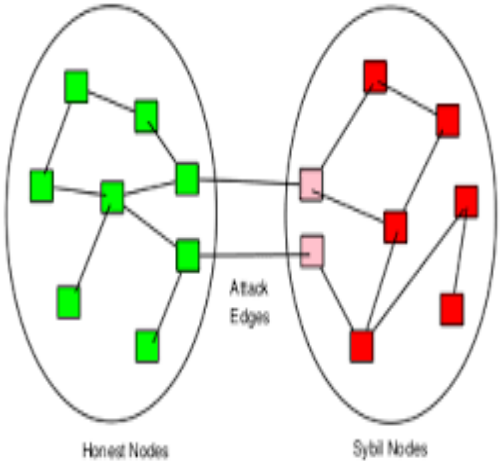


Fig. 4. Attacks by Sybil nodes

SybilInfer shows how robust Sybil defenses can be bootstrapped from distributed trust judgments, instead of a centralized identity strategy. This is a key enabler for secure peer-to-peer architectures as well as collaborative web applications. SybilInfer is also significant because it makes use of machine learning techniques and their careful application to a security problem. The ability to demonstrate that the underlying mechanisms behind SybilInfer is not susceptible to foolery by an adversary organizing its Sybil nodes in a particular topology is, in this aspect, a very important part of the SybilInfer security design.

2.2. Limitation

This algorithm cannot distinguish the honest nodes from the Sybil nodes without providing a cutoff point.

3. SYBIL LIMIT

There is always a huge threat to open-access distributed systems like peer-to-peer systems from Sybil attacks, where an ill-willed user creates many fake identities known as Sybil nodes. Unless a reliable central authority is organized which bonds identities to real persons, safeguarding against Sybil attacks is a serious problem. Amidst the limited dispersed approaches, a recent protocol called SybilGuard uses a key perception on social networks to restrict the number of Sybil nodes that are acknowledged. In spite of its encouraging efforts, SybilGuard can permit many number of Sybil nodes to be acknowledged. Moreover, SybilGuard believes that social networks are fast-mingling, which has not been accepted in the actual world. Here we deal with the SybilLimit [9] protocol that uses the similar perception as SybilGuard, but provides a refined and close to reality results.

In a trial for a million-node system, the number of Sybil nodes acknowledged is decreased by a factor or about 200 times using SybilLimit protocol.

Ultimately, on the basis of three large-scale real-world social networks, the most important proof that real-world social networks are really fast-mingling has been offered by SybilLimit.

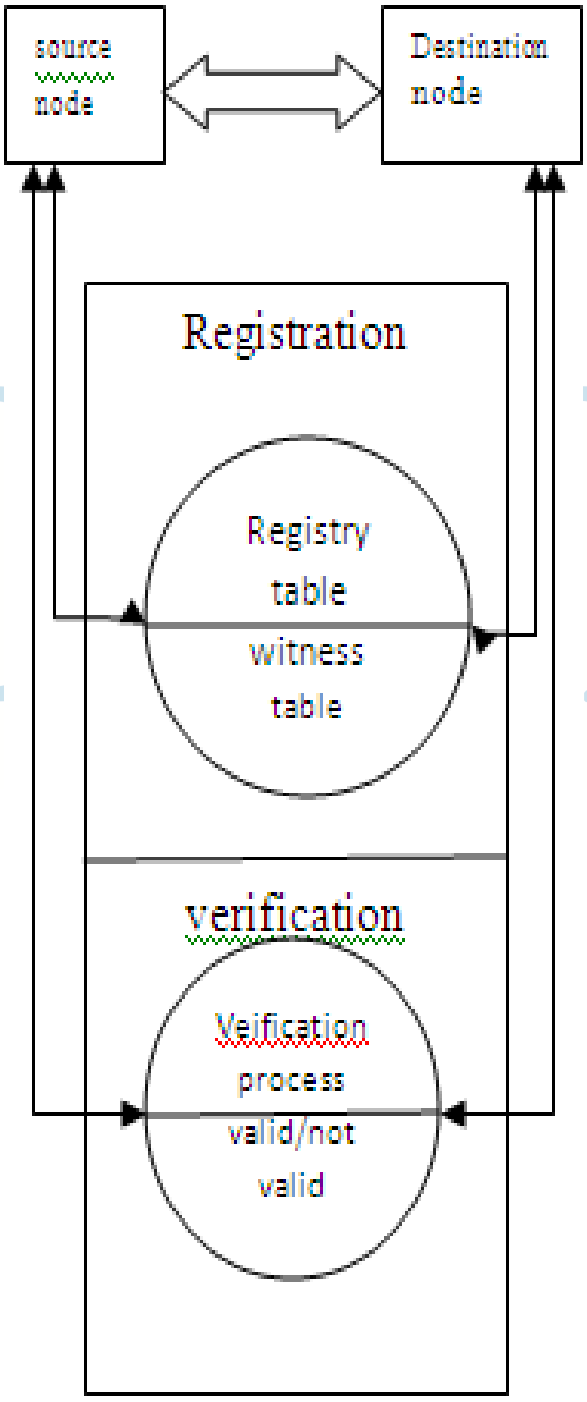


Fig. 5. Sybil limit protocol

3.1. Assumptions of SybilLimit

- Established social network G (n, m) which is unstructured undirected fast-mixing: mixing time O (log N).
- Sybils penetrate the network through attack edges.
- Nodes are identified by their public keys.

3.2. Sybil attacks

- Each honest node knows only its neighbors.
- Sybils know the entire graph.
- Sybils try to slip into the honest zone by fooling the verifiers.

3.3.Basic operation in SybilLimit

- Takes a random route on SybilLimit.
- Uses one-to-one mapping from incoming edges to out coming edges.
- fixed length w=O(log n).
- The head is registered by the tail node.
- The new head rewrites old head for a single tail.

SybilLimit is efficient because, for a given tail, the route led to it is determined. There are no more routes that end up with the same tail.

Sybil limit, a near-optimal defense against Sybil attacks using social networks and the goal of Sybil limit is limiting the number of accepted Sybil nodes. SybilLimit leverages multiple independent instances of the random route protocol(as shown in Fig.5) to perform many short random routes and exploiting intersections on edges instead of nodes and using the novel balance condition to deal with escaping tails of the verifier.

In future, going to implement neighbor node against Sybil node. In that we are going to add registration table for neighbor nodes that will provide the tokens for our honest nodes. The tokens are used for security purpose. If the keys are valid by the registration table, then the communication is done. If the keys are not valid by the registration table, the communication is not done. Then the invalid node is said to be Sybil node. The Sybil node is thrown out of the network. Sybil limit will sincerely limits the Sybil node while comparing to the existing systems. The bounding of the Sybil node will be under O (log n).

3.4.Limits of SybilLimit

- Uses an undirected unweighted graph.
- Assumes that an honest network exists already – no bootstrap stage.
- Favorable to newcomers with many links but is unfavorable to those with few links.
- Demands that the network must be fast mixing

4. SYBIL RESILIENT

A Sybil-resilient [10] is a vote aggregation system that leverages the trust network among users to defend against Sybil attacks. SumUp uses the adaptive vote flow aggregation technique to limit the number of bogus votes cast by adversaries, such that the number of votes cast is lesser than the number of attack edges in the trust network (with high probability). Sybil-resilient uses a protocol called SumUp. Using user feedback on votes, SumUp restricts the voting power of adversaries who misbehave continuously to below the number of their attack edges. By carefully evaluating several existing social networks such as YouTube, it is possible to conclude that SumUp has the ability to handle Sybil attacks.

4.1. SumUp Vote Aggregation

SumUp [11] enhances the trust relationship that exists already among users. In view of human efforts taken to establish a trust link, the attacker is unlikely to possess many attack edges. SumUp addresses the vote aggregation problem which can be stated as follows: Given n votes on an object, of which a random fraction may be from Sybil identities created by an attacker, how would we collect votes in a Sybil resilient manner?

Sybil-resilient vote aggregation solution should satisfy three properties:

- Firstly the solution should collect a significant fraction of votes from honest users.
- Secondly if the attacker has attack edges, the maximum number of bogus votes should be bounded by, independent of the ability of the attacker to create many Sybil identities behind him.
- Thirdly if the attacker repeatedly casts bogus votes, his voting ability in the future should be minimized. SumUp achieves all three properties with high probability in the face of Sybil attacks

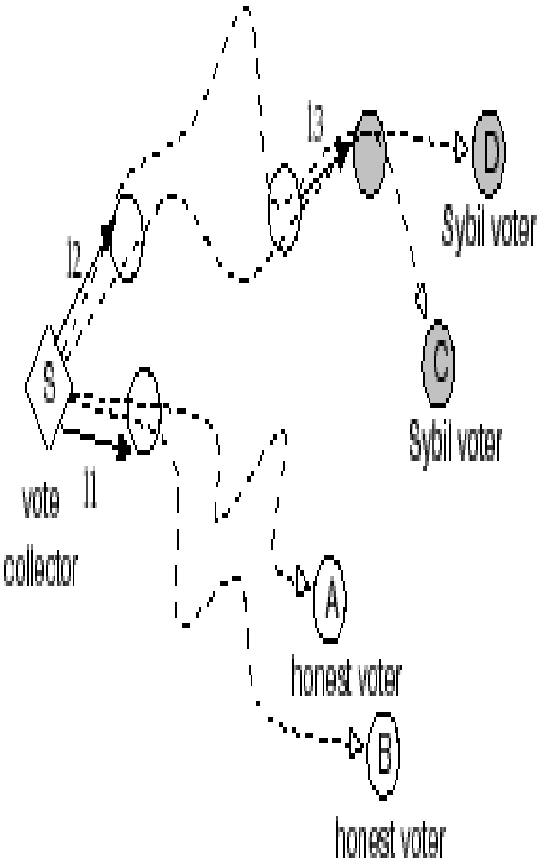


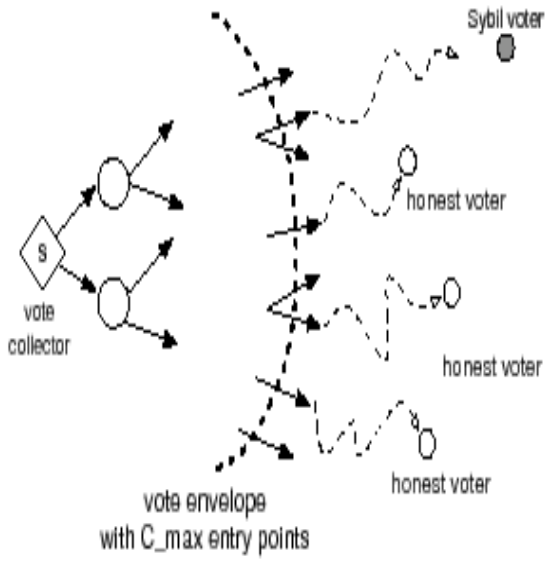
Fig. 6. SumUp computes a set of approximate max-flow paths from the vote collector S to all voters (A, B, C, D). Straight lines denote trust links and curly dotted lines represent the vote flow paths along multiple links. Vote flow paths to honest voters are ``congested" at links close to the collector while paths to Sybil voters are also congested at far-away attack edges.

The idea behind SumUp is to achieve adaptive vote flow technique as shown in Fig.6. which appropriately assigns and alters link capacities in the trust graph to collect the net votes for a given object.

The instinctive knowledge behind adaptive vote flow helps SumUp address the vote aggregation problem. This approach assigns link capacities to bind the attack capacity of an attacker.

4.2. Flow-based vote Aggregation

A flow-based vote aggregation system faces the tradeoff between the maximum number of honest votes it can collect and the number of potentially bogus votes collected



.Fig. 7. Through ticket distribution, SumUp creates a vote envelope around the collector. The capacities of links beyond the envelope are assigned to be one, limiting the attack capacity to be at most one per attack edge for adversaries outside this envelope.

III. CONCLUSION

Most of the peer-to-peer systems are prone to Sybil attacks. In this paper, we have discussed the Different techniques to defend Sybil attacks that can be applied on various application domains. Finally and most importantly, no actual working protocol to defend against Sybil attacks has yet been built. These preliminary protocols have significant drawbacks which we need to overcome.

IV. REFERENCES

1. J. R. Douceur, "The Sybil attack," in Proc. of IPTPS, March 2002
2. S. Murphy, "Teens ditch e-mail for texting and facebook," MSNBC.com, Aug 2010.
3. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in Proc. of IMC, 2010
4. C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: the underground on 140 characters or less," in Proc. of CCS, 2010.
5. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in Proc. of SIGCOMM, 2006.
6. B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based sybil defenses," in Proc. of SIGCOMM, 2010.
7. G. Danezis and P. Mittal, "Sybilinfer: Detecting sybil nodes using social networks," in Proc of NDSS, 2009.
8. Q. Lian, Z. Zhang, M. Yang, B. Y. Zhao, Y. Dai, and X. Li, "An empirical study of collusion behavior in the maze p2p file-sharing system," in Proc. of ICDCS, June 2007
9. H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: A nearoptimal social network defense against sybil attacks," in Proc. of IEEE S&P, 2008.
10. Xu Xiang Coll. of Inf. Eng., China Jiliang Univ., Hangzhou, China ; Zhou Hangxia "A Sybil-Resilient Peer-to-Peer Network Protocol",2008.
11. N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-resilient online content voting," in Proc. of NSDI, 2009.