Sybil Clutches: Apprehension and Attestation

Prof. Nidhi Sharma[1] Ashwini A. Dange[2] Monali M. Kamthe[3] Swapnil S. Menge[4]
[1, 2, 3, 4] Student, Computer Engineering Department
[1, 2, 3, 4] Bharati Vidyapeeth College of Engineering, Maharashtra, India

Abstract---Sybil attacks are one of the well-known and powerful attacks against online social networks. Sybil users propagate spam or unfairly increase the influence of target users. However, sybil users alone do not harm the system. What is really dangerous that multiple sybil users collude together and form a sybil clutch. In this paper, we present the first attempt to identify and validate sybil clutches in online social networks. We build sybil clutch detector based on multiple attributes such as based on last login time, register time, friend establishment time etc. Our sybil clutch apprehension and attestation mechanisms have important implications for system design to defend against sybil attacks in online social networks.we verify that the largemajority of links between Sybil accounts are created accidentally, unbeknownst to the attacker.

I. INTRODUCTION

Sybil accounts are hoax identities created to unfairly increase the power or resources of a single malicious user. Recently, online social networks (OSNs) have also come under attack from Sybils. Researchers have observed Sybils forwarding spam and malware on Facebook and Twitter, as well as infiltrating social games. Looking forward, Sybil attacks on OSNs are poised to become increasingly. According to research on sybil clutch detector to Renren, they identify 2,653 sybil clutches and 989,764 sybil users. Existing Distributed systems are ill-equipped to defend against this attack, since determining a tight mapping between real users and online identities is an open problem. To date, researchers have demonstrated the efficacy of Sybil attacks against P2P systems, anonymous communication networks, and sensor networks.

Sybil account activity in Renren, the largest OSN in China. In Section 2, they used ground truth data on Sybils provided by Renren Inc. to characterize Sybil Behaviour & identied several behavioral attributes that are unique to Sybils, and leverage them to build a measurement based, real-time Sybil detector. Sybil detector is currently deployed on Renren's production systems, and between August 2010 and February 2011 it led to the identification and banning of over 100,000 Sybil accounts.

In summary, we present the first attempt to identify and validate sybil clutches in online social networks. We utilize multiple attributes to detect sybil users and identify sybil clutches in the real system. Our results are confirmed by automatic attestation mechanisms, instead of simulation experiments or manual inspections. Our sybil clutch apprehension and attestation mechanisms have important implications for system design to defend against sybil attacks in OSNs. Our analysis of Sybil behavior and characteristic demon-strates that existing Sybil defenses are unlikely to succeed on today's OSNs. This opens the door for the development of new techniques to effectively detect and defend against Sybil attacks.

This module is used for the apprehension of the Sybil clutches in the system. The application takes into consideration the user registration time, login time and the activities perform. The module also tracks the rate at which a particular user adds friends in the system along with their activities. If a system after considering all the factors considers that the user is a Sybil, then it automatically checks the peers in the list. If the maximum peers are Sybil, then the system automatically recognizes the clutch as a Sybil clutch and notifies the admin.

To effectively attract friends and disseminate advertise-ments, most Sybil accounts on Renren blend in extremely well with normal users. They tend to have completely filled user profiles with realistic background information, coupl ed with attractive profile photos of young women or men, mak-ing their apprehension quite challenging.

First of all, we identify suspicious users and summarize the implementation in algorithm 1. The initial set of suspicious users consists of people who have the popularity smaller than 10, and the social degree bigger than 20. In the subsection II-B, we observe that normal users have the popularity at least equal to the social degree

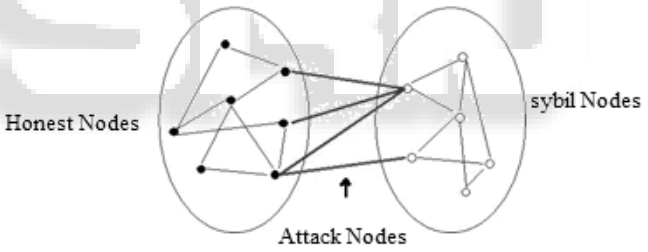

Figure. 1: The social network with honest nodes and sybil nodes. Note that regardless of which nodes in the social net-work are sybil nodes, we can always "pull" these nodes to the right side to form the logical network in the figure.

However, the attacker easily controls some sybil users to send friend requests, and manipulate other sybil users to accept friend requests. Sybil users do not need to view others' profiles in the establishment of social relationships, and their popularity is smaller than the social degree. Then we filter out suspicious users with loose relationships with other suspicious users. For every suspicious user, we compute the number of friends who are also in the suspicious set. If the user has less than 5 suspicious friends, the user is deleted from the suspicious user.

Algorithm 1: Identification of suspicious users.
Input:

U: the set of all users

popularityi: the popularity of the user i (i ∈ U)
socialDegreei: the social degree of the user i (i ∈ U)
Fi: the set of user i's friends (i ∈ U)
S: the set of suspicious users

Procedure:

1) S = φ
2) for i ∈ U do
3) if popularityi <= 10 then
4) if socialDegreei >= 20 then
5) S = S ∪ {i}
6) end if
7) end if
8) end for
9) for i ∈ S do
10) if |Fi ∩ S| < 5 then
11) S = S − {i}
12) end if
13) end for
14) for i ∈ U\S do
15) if |Fi ∩ S| > 0.5 ∗ |Fi| then
16) S = S ∪ {i}
17) end if
18) end for
19) return S;

These people blend in well with normal users, but they are still suspicious. We add users into the suspicious set, who have more than 50% of abnormal friends. Secondly, we divide suspicious users into sybil clutches. We utilize IP addresses when users register their accounts. If suspicious users are registered with similar IP addresses, they are likely to be controlled by the same attacker. We classify suspicious users based on prefixes of their IP addresses. For example, the suspicious user has the IP address as A.B.C.D. We extract the prefix as A.B, and put the user into the corresponding clutch. All suspicious users are divided into clutches by their IP addresses. Attackers often create many sybil users and control them to collude together. Small clutches are useless for attacks. So we filter out clutches with less than 5 users. Remaining clutches are identified as sybil clutches, and people in these clutches are considered as sybil users.

A. Apprehension Results

We apply our sybil clutch detector to Renren, and identify 2,653 sybil clutches and 989,764 users. The largest Sybil clutch has the size 38,994. We classify sybil and users in Table I.For clutches with the size between 6 and 10, they cover 11.4% of clutches and 0.2% of users. 39.3% of clutches have the size between 11 to 100, and 41.3% of clutches have the size between 101 to 1,000. The majority of clutches have medium size. 43.8% of users belong to large clutches with the size between 1,001 and 10,000. Only 6 clutches have the size bigger than 10,000, but these clutches have 128,481 users in total. Large sybil clutches are extremely dangerous in online social networks. If all users in a large sybil clutch collude together, they can harm the system seriously.

II. VALIDATING SYBIL CLUTCHES

Given the lack of publicly available datasets, previous works [9], [10], [11], [12] use simulation to evaluate their methods. However, simulation experiments consider several important factors, and ignore other factors. It is still unknown about the performance of these methods in real systems. In order to assess their methods, Tran et al. manually inspect suspicious articles [12], and Yang et al. examine feedback from customer support department [13]. These techniques require much human effort, and they are effective only after suspicious articles have been posted or abnormal users have been forbidden.

In this section, we design automatic mechanisms to vali-date our sybil clutch detector. We study action time similarity of users in sybil clutches, in comparison with normal clutches. In order to build normal clutches, we randomly select 200,000 users from 200 universities. We use the same technique in subsection II-C, and divide users into clutches based on prefixes of IP addresses. Then we filter out clutches with less than 5 users, and identify remaining clutches as normal clutches. Since people in the same university are likely to have similar IP addresses, the majority of clutches have more than 5 users. Overall, we obtain 1,480 normal clutches and 179,319 normal users.

A. Attestation Methodology

To validate sybil clutches, we use the widely acknowledged distinguishing feature: the action time similarity. The action time similarity is based on the intuition that all users in a sybil clutch take coordinated actions within the similar time. For example, many users post spam in a short time in Facebook, and their posting time is similar [3]. In order to save the time cost, the attacker simultaneously controls all users in a sybil clutch to take actions.

We utilize the median interval of action time to measure the similarity. We summarize the computation of median interval in algorithm 2.

Algorithm 2: Computation of median interval of action time.

Input:

G: the set of all users in a clutch

actionT imei: the action time of the user i (i ∈ G)

m: the median interval of action time for a clutch.

Procedure:

1) n = |G|
2) sort actionT imei for all users in a clutch, and output results as actionT imei_ (actionT ime1_ < actionT ime2_ < ... < actionT imen_)
3) for each i ∈ [1, n − 1] do
4) intervali = actionT ime(i+1)_ − actionT imei_
5) end for
6) sort intervali and output results as intervali_ (interval1_ < interval2_ < ...interval(n−1)_)
7) m = interval[n/2]_
8) return m;

Firstly, we sort action time of all users in a clutch. Then we measure the absolute time interval between consecutive actions, and extract the median value of all such intervals. If users take actions within the short time, their action time is similar and the median interval is small; if users randomly take actions within the long time, their action time is dissimilar and the median interval is large.

The median interval characterizes the time similarity of actions taken by all users in a clutch. However, the median interval is negatively correlated with the clutch size. The bigger the clutch is, the more intensively user actions are distributed in the time period, which causes the smaller median interval. In contrast, the small clutch is

likely to have the large median interval. In order to reduce the impact of the clutch size, we multiply the median interval by the clutch size.

We define three attestation methods:

1) The attestation based on register time:

The register time is defined as the time when the user registers a new account in the system. For a clutch, we compute the median interval of register time multiplied by the clutch size. If the value is much smaller than that of a normal clutch, the register time of users are distributed too intensively, and we validate the clutch as the sybil clutch.

2) The attestation based on last login time:

The last login time describes the time when the user logins into the OSN for the last time. For a clutch, we compute the median interval of last login time multiplied by the clutch size. If the value is much smaller than that of a normal clutch, users in the clutch login in clutch with the similar time, and the clutch is validated as the sybil clutch.

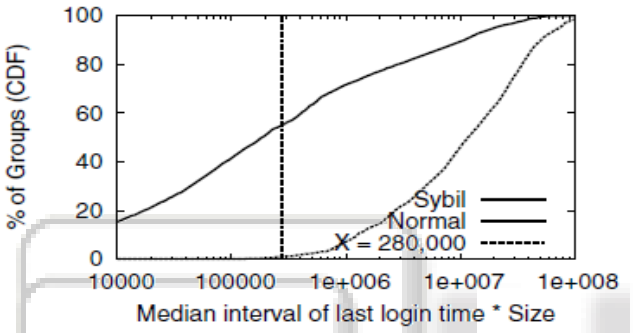

Figure 2. Group distribution of sybil groups and normal groups

user establishes the social relationship with a friend. For a clutch, we compute the median interval of friend establishment time multiplied by the number of friend relationships. Note that we mainly consider friend relationships within the clutch. The attacker simultaneously controls sybil users to make friends with others in the same clutch.

3) The attestation based on friend establishment time:

The friend establishment time describes the time when the, establishment time of social relationships within the clutch is likely to be similar. Sybil users also send friend requests to normal users outside of their clutch. The friend establishment time is determined by normal users, instead of attackers. If the result is extremely smaller than that of a normal clutch, social relationships within the clutch are established within the short time, and their clutch is validated as the sybil clutch.

B. Attestation Results

First of all, we apply the attestation based on last login time to verify sybil clutches detected in the subsection II-D. For each clutch, we compute the value of the median interval of last login time multiplied by the clutch size. Figure 2 shows the clutch distribution of sybil clutches and normal clutches. 55.2% of sybil clutches have the value smaller than 280,000, while only 1% of normal clutches have the value smaller than 280,000. We further consider the number of users in clutches and plot user distribution in Figure 3. 63.1% of sybil users are in clutches with the value smaller than 280,000, while 0.24% of normal users are in clutches with the value smaller than 280,000. Consequently, 55.2% of sybil clutches have much smaller value than that of normal clutches. Users in these clutches show obvious similarity of last login time, and they are simultaneously controlled by attackers. 1464 (55.2%) sybil clutches are successfully validated.

We also apply attestation methods based on register time and friend establishment time, respectively. If the clutch is validated by at least 1 attestation method, the clutch is successfully verified. Table II show the number of sybil clutches and sybil users, who are successfully verified by 1, 2 or 3 of attestation methods, respectively. Overall, 2440 (91.9%) sybil clutches and 985,797 (99.6%) Sybil users are successfully validated. 31.8% of sybil clutches and 54.4% of sybil users are even validated by 3 methods. Results show that our sybil clutch detector achieves good performance.

III. MEASURING SYBIL CLUTCHES

We measure the topological characteristics of sybil clutches validated in the section III. In particular, we analyze how sybil clutches connect to normal users in the wild. Following the definitions proposed in previous works [11], [13], attack edge is defined as the social relationship between a sybil user and a a normal user. We begin measurement of sybil topology by examining the attack edges of sybil clutches in Renren. For every sybil clutch, we compute the number of attack edges with normal users. Then we plot results of all sybil clutches in Figure 4. Only 15% of sybil clutches have less than 100 attack edges; 40% of sybil clutches have more than 1,000 attack edges. Some of sybil clutches build a large number of social relationships with normal users. We take a further step, and compare attack edges and all edges. For each sybil clutch, we calculate the number of attack edges divided by the number of all edges. Figure 5 shows the percentage of attack edges. 28% of sybil clutches have less than 10% of attack edges. Users in these sybil clutches seldom build social relationships with normal users. These sybil users are still harmful to the system, because they can spread advertisements by leaving comments in target users' profiles. In contrast, 24% of sybil clutches have more than 30% of attack edges, and 9% of sybil clutches have more than 50% of attack edges. A large number of friend relationships are built between sybil users and normal users in these clutches. Previous apprehension algorithms [9], [10], [11], [12] identify sybil users by locating the small number of edge cuts that separate the sybil users from normal users. Since some sybil clutches have a large percentage of attack edges, previous apprehension algorithms are unlikely to succeed on social graphs. This opens the door for the improvement of apprehension algorithms to consider more trustful graphs.

IV. CONCLUSION

In this paper, we present the first attempt to identify and validate sybil clutches in the real system. First of all, we build the sybil clutch detector based on multiple attributes, including popularity, social degree, friend relationship and IP address. We apply the sybil clutch detector to Renren, and identify 2,653 sybil clutches and 989,764 sybil users. Secondly, we design automatic attestation mechanisms of

sybil clutches, by analyzing action time similarity of users in a clutch. Overall, 2440 (91.9%) sybil clutches and 985,797 (99.6%) sybil users are successfully validated. Our sybil clutch apprehension and attestation mechanisms have important implications for system design to defend against sybil attacks in OSNs

REFERENCES

[1] Bauer, K., Mccoy, D., Grunwald, D., Kohno, T., And Sicker, D. Low-Resource Routing Attacks Against Tor. In Proc. Of Workshop On Privacy In Electronic Society (Alexandria, Va, 2007).
[2] Benevenuto, F., Magno, G., Rodrigues, T., And Almeida, V. Detecting Spammers On Twitter. In Proc. Of Ceas (Redmond,Wa, July 2010).
[3] Danezis, G., And Mittal, P. Sybilinfer: Detecting Sybil Nodes Using Social Networks. In Proc Of Ndss
[4] Douceur, J. R. The Sybil Attack. In Proc. Of Iptps(March2002)
[5] Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., And Zhao, B. Y. Detecting And Characterizing Social Spam Campaigns. In Proc. Of Imc (2010).
[6] Grier, C., Thomas, K., Paxson, V., And Proc. Of World Wide Web Conference (Raleigh, Nc, April 2010).
[7] Kwak, H., Lee, C., Park, H., And Moon, S. B. What Is Twitter, A Social Network Or A News Media? In Proc. Of World Wide Web Conference (Raleigh, Nc,April 2010).
[8] Lenhart, A.,Purcell, K.,Smith A, And Zickuhr, K. Social Media And Young Adults
[9] Lian, Q., Zhang, Z., Yang, M., Zhao, B. Y., Dai, Y., And Li, X. An Empirical Study Of Collusion Behavior In The Maze P2p File-Sharing System. In *Proc. Of Icdcs* (June 2007).
[10] Murphy, S. Teens Ditch E-Mail For Texting And Facebook.Msnbc.Com, Aug 2010.
[11] Nazir, A., Raza, S., Chuah, C.-N., And Schipper, B. Ghostbusting Facebook: Detecting And Characterizing Phantom Profiles In Online Social Gaming Applications. In *Proc. Of Sigcomm Wosn* (June 2010).
[12] Newsome, J., Shi, E., Song, D., And Perrig, A.The Sybil Attack In Sensor Networks: Analysis Defenses. In *Proc. Of Ipsn* (Berkeley, Ca, 2004).
[13] Sophos. Sophos Facebook Id Probe Shows 41% Of Users Happy To Reveal All To Potential Identity Thieves. Http://Www.Sophos.Com/Pressoffice/News/Articles/2007/8/Facebook.Html,2007.
[14] Stringhini, G., Kruegel, C., And Vigna,G. Detecting Spammers On Social Networks. In *Proc. Of Acsac* (Austin, Tx, December 2010).
[15] Tran, N., Min, B., Li, J., And Subramanian, L.Sybil-Resilient Online Content Voting. In *Proc. Of Nsdi* (2009).

