Recent Trends in Sybil Attacks and Defense Techniques in Social Networks

Snehal Pise
G.S.Moze College of Engineering, Balewadi, Pune-45.
University Of Pune, Pune, India.

Prof. Ratnaraj Kumar
G.S.Moze College of Engineering, Balewadi, pune-45.
University Of Pune, Pune, India.

Abstract

Decentralized distributed systems or Peer-to-peer systems are particularly vulnerable to sybil attacks. In Sybil attack, an adversary or a malicious user gets multiple fake identities pretending of new distinct nodes in the system. Controlling large number of nodes in the system, malicious user is able to out vote the genuine users.
In this paper various types of sybil attacks are explained which are based on behaviour of attacker, which also enables us to better understand the threats posed by each type of attack. This paper also surveys different types of current sybil defense protocol techniques like SybilGuard, SybilShield, SybilLimit, SybilDefender and SyMon to defend against the Sybil attack. These protocol techniques are based on the "social network" among user identities where an edge between two identities indicates a human-established trust relationship. In this paper these techniques are described and compared with each other.

Keywords– Sybil attack, Sybil Guard, Sybil Limit, Sybil Shield, Sybil Defender

1. Introduction

Sybil attack is an attack on computer system or network in which an adversary creates as multiple fake identities, pretends as different entities, and then launches attacks through these fake identities. Such identities itself often becomes untraceable.

This threat is particularly acute in decentralized systems, where it may be impractical or impossible to rely on a single authority to certify which users are legitimate [6]. Sybil attacks in which an adversary forges a potentially unbounded number of identities are a danger to distributed systems and online social networks. With Sybil nodes compromising a large fraction of remaining nodes in the system, the adversary is able to take control of the system.

With Sybil nodes comprising a large fraction (e.g., more than 1/3) of the nodes in the system, the malicious user is able to "out vote" the honest users, effectively breaking previous defenses against malicious behaviours [3]. Thus, an effective defense against Sybil attacks would remove a primary practical obstacle to collaborative tasks on peer-to-peer (p2p) and other decentralized systems. Such tasks include not only Byzantine failure defenses, but also voting schemes in file sharing, DHT routing, and identifying worm signatures or spam.

In their research paper [8], Wei Chang et al. have specified three examples. First, in some distributed systems, critical resources are assigned based on the voting results of participants: usually, only the node that has received the highest number of votes can access resources. If attacker illegally creates many Sybil identities, then adversary may proportion more resources by instructing the fake identities to vote in firm ways, such as always voting for her fake identities. Since distributed system, the research works on Sybil defense techniques hold the most important position votes are collected indirectly; it is hard to detect the illegitimate votes.

Another example comes from an application of sensor networks called persistent temperature monitoring. It

has found that multiple sensors are randomly and uniformly deployed in a large region. Each sensor measures temperature around it, and then forwards the readings to its sink node, which collects the data. With the help of sink node, an average temperature is calculated. But if the attackers commence Sybil attacks and allows each Sybil identity to report one more temperature degree, then the average temperature result will be definitely incorrect.

Third example comes from a Facebook vote application. Here if an enemy maliciously creates many more identities, she can easily change the overall popularity of an option by providing plenty of false praise, or bad mouthing of the option through Sybil identities. As it is clear that false opinions of the Sybils may change final decision of any distributed system, the research works on Sybil defense techniques hold the most important position.

2. Categories of Sybil Attacks

There are three broad categories of Sybil attack.

2.1. Direct vs. Indirect Communications

James Newsome et al. have mentioned different categories of sybil attacks [7]. How Sybil nodes communicate with honest nodes is also a significant consideration during the designing of Sybil defense mechanisms. The attacker can directly communicate with an honest node by using one of her Sybil identities, or she can use only her own real identity for communicating with all others, and then route the Sybil data through this real identity. For the attackers, the easiness of direct communication with honest nodes directly influences the success of attacking. In general, the attackers with much more direct communications are much more difficult to detect. However, for few distributed systems, it is difficult to have direct communication.

In Direct Communication type attack, the Sybil nodes communicate directly with legitimate nodes. When a legitimate node sends a radio message to a Sybil node, there is possibility of listening message by one of the malicious devices. Similarly, messages which are sent from Sybil nodes are in reality sent from one of the malicious devices.

In Indirect Communication attack, no legitimate nodes are able to communicate directly with the Sybil nodes. Instead, one or more of the malicious devices claims to be able to reach the Sybil nodes. Messages sent to a Sybil node are actually routed through one of these malicious nodes, which pretends to pass on the message to a Sybil node.

2.2. Simultaneous vs. Non-Simultaneous

The attacker can obtain all of her Sybil identities concurrently, or she can even generate them one-by-one. For an intelligent attacker, the more diverse features the Sybil nodes have, it is harder to identify Sybil nodes. Gradually creating Sybil nodes may potentially differentiate the first appearing time of the Sybil. However, the process may delay time of attack, and therefore increases the blast time of some Sybil. If a distribution randomly checks the authentication of some identities, there is a higher chance of being caught to previously generated identities.

In Simultaneous attack, the attacker may try to have his Sybil identities all participate in the network at once. A particular hardware entity can only act as one identity at a time, it can also cycle through these identities to make it appear that they are all present simultaneously.

In Non-Simultaneous attack, the attacker might present a large number of identities slowly over a period of time, somehow only acting as a small number of identities at any given time. The attacker can do this by having one identity seem to leave the network, and have another identity join in its place. A particular identity might leave and join multiple times, or the attacker might only use each identity once. Another possibility is that the attacker could have several physical devices in the network, and could have these devices exchange their identities. As the number of identities the attacker uses is equal to the number of physical devices, so each device presents different identities at different times.

2.3. Fabricated vs. Stolen Identities

A Sybil node can get an identity either as a brand new identity, or an identity stolen from a legitimate node. In Fabricated Identities, the attacker can simply create arbitrary new Sybil identities. For instance, if each node is identified by a 32-bit integer, the attacker can simply assign each Sybil node a random 32-bit value. In Stolen Identities, given a mechanism to identify genuine node identities, an attacker cannot produce new identities. For example, suppose the name space is intentionally limited to prevent attackers from inserting new identities. In this case, the attacker needs to assign other legitimate identities to Sybil nodes. This identity

theft may go undetected if the attacker destroys or temporarily disables the impersonated nodes. A related issue is identity replication, in which the same identity is used many times and exists in multiple places in the network. The identity replication attack can be performed and defended against independently of the Sybil attack [7].

The Sybil attacks can also be classified based on the several characteristics of the attacker:

2.4. Insider vs. Outsider

Whether an attack is an insider or outsider directly determines the capability of the attacker, and the inflexibility of inducing a Sybil attack. Attacker holds at least one genuine identity for an insider and claims that as if she receives certain data from the other nodes, and that is by using the fake identities. Distributed system assumes that each node is honest and therefore assumes that the false data can be easily forwarded to the whole system. However, for an outsider, she is any illegal or say dishonest entity; before launching or inducing a Sybil attack, she needs to first access the system. But, distributed systems uses some kind of authentication to prevent illegal access, for example, entering a password, data encryption. The outsider requires understanding of all the mechanisms of the system prior to launching Sybil attacks. That is why distributed systems are more susceptible to inside attackers [8].

2.5. Selfish vs. Malicious

For security-related problems, there are two different types of attackers: either selfish or malicious. Selfish attackers manipulate the false data just for their own advantage, while malicious attackers attempt to threaten or weaken a system[8]. Whether an attacker is selfish or malicious is usually determined by the different types of targeted distributed system and also by final attacking effects. For instance, in the previous critical resource accessing example, if the attacker has resource accessing rights all to her, then definitely she is a malicious attacker, because others cannot use the resource. However, if other users can also access the resource with a smaller amount of probability, then she is selfish attacker. Because malicious attacks usually have much more serious effects, it is of greater importance to protect against potentially malicious attacks than that of potentially selfish attacks.

2.6. 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 [8]. Essentially, the selection of these two schemes is determined by how inexpensive it is to obtain an identity. If the attacker can very easily get ample of fake identities, some Sybil nodes that are idle could make them more real, as an honest node may leave or re-enter the system many times. However, the power of Sybil attacks results from the number of the identities. Obtaining a large number of identities is if very difficult, then the attacker must use all of them in order to launch or induce a successful attack.

2.7. Discarded vs. Retained

For an attacker, managing of old Sybil identities is really necessary. After locating a Sybil node, further one can identify the others by monitoring the claimed communication between a suspect node and the detected Sybil node. Because 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 reject them. Assume that generating Sybil identities has some costs, and the naming space is not infinite. The capacities of attacks are related with the naming costs and the mechanism of using old identities [8].

3. Defense Mechanism against Sybil Attacks

To protect against these Sybil attacks, it is necessary to validate that each node identity is the only identity presented
by the corresponding physical node. There are two types of ways to validate node identity. The first type is called direct validation, in which a node directly tests if another node's identity is valid. The second type is called indirect validation, where nodes that have already been verified or checked are allowed to assure for or prove false other nodes. With the exception of the key pool defense, the mechanisms that we present here are for direct validation. We leave secure methods of indirect validation as future work.

3.1. SybilGuard

Haifeng Yu, et al. in their research paper have introduced SybilGuard[3]. SybilGuard is a novel decentralized protocol for reducing the bad influences of sybil attacks, by bounding both the number and size of sybil groups. This protocol is based on the "social network"

between user identities, where an edge between two identities specifies a human-established trust relationship. Even though malicious users can create many identities but they can have few trust relationships [3]. Therefore, we see a disproportionately small "cut" in the graph between the honest nodes and the Sybil nodes. SybilGuard makes use of this property to bind the number of identities a malicious user can create. SybilGuard relies on these properties of the users' underlying social network, namely that (i) the honest region of the network is fast mixing, and (ii) malicious users may create many nodes but relatively few attack edges. In all its simulation experiments with one million nodes, SybilGuard ensured that (i) the number and size of sybil groups are properly bounded for 99.8% of the honest users, and (ii) an honest node can accept, and be accepted by, 99.8% of all other honest nodes.
The current SybilGuard design relies on the fast mixing property of social networks. If the social network is not fast mixing, SybilGuard will still properly bound the number of accepted sybil nodes within with high probability. The main drawback of a slower mixing social network is that more honest nodes will be mistakenly rejected [3].

SybilGuard Design works in four steps

A. Social Network and Attack Edges: SybilGuard leverages the existing human-established trust relationships among users to bound both the size and number of Sybil groups. Here exactly all honest nodes and sybil nodes in the system form a social network see in Fig. 1 [3]. An undirected edge exists between two nodes if the two corresponding users have strong social connections (e.g., colleagues or relatives) and trust each other not to launch a sybil attack. If two nodes are connected by an edge, we can say for sure that the two users are actually friends. It should be noted that here the edge indicates strong trust, and the notion of friends is quite different from friends in other systems such as online chat rooms. An edge may exist between a sybil node and an honest node if a malicious user let Malory successfully fools an honest user Alice into trusting her. Therefore this edge is called an attack edge and we use to denote the total number of attack edges [3]. With the help of authentication mechanism, SybilGuard ensures that regardless of the number of sybil nodes Malory creates, Alice will share an edge with at most one of them as in the real social network. Thus, the number of attack edges is limited by the number of trust relation pairs that the adversary can establish between honest users and malicious users.

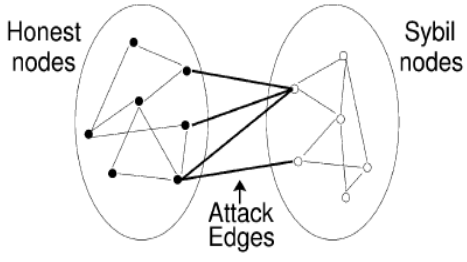

Figure 1. The social network with honest nodes and sybil nodes.

Note that regardless of which nodes in the social network are Sybil nodes, we can always "pull" these nodes to the right side to form the logical network in the figure.

B. Random Routes: SybilGuard uses a special type of random walks in the social network called as random routes. In the standard kind of random walk at each hop the current node selects a uniformly random edge to direct the walk. In random routes, each node uses a pre-computed random permutation as a one-to-one mapping from incoming edges to outgoing edges [3]. Specifically, each node uses a randomized routing table to decide the next hop. Assume a node A with d neighbours uniformly randomly chooses a permutation "x1, x2, ... , xd" among all permutations of 1,2,...d. If a random route comes from the ith edge, A uses edge xi as the next hop. It is possible that i = xi for some i. The routing table of A, if chosen once then that will never change.

C. Route Intersection as the Basis for Acceptance: In SybilGuard, a node with degree d performs d random routes (starting from itself) of a certain length w one along each of its edges. These random routes form the basis of SybilGuard whereby an honest node (the verifier V) decides whether or not to accept another node (the suspect S). In particular, a verifier route accepts S if and only if at least one route from S intersects that route from V. V accepts if and only if at least a threshold of 's routes accept S [3].
D. Secure and Decentralized Design for Random Routes and Their Verification

3.2. SybilShield

SybilShield, a novel decentralized defense protocol against Sybil attacks in multi-community social networks, which limits the negative influences of accepting Sybils mistakenly and mislabelling honest

nodes [1]. SybilShield is based on underlying properties of real-world social networks that the non-Sybil regions are fast mixing and the number of attack edges created by an adversary is relatively less than that of foreign edges among honest communities, which are validated on the given MySpace topology data sample. Inspired by these social network properties, we introduce agents for help if the initial validation by performing random routes denies to accept the suspect node. Through the theoretical probability analysis and experiments on the MySpace data set, SybilShield is shown to greatly outperform SybilGuard, reducing the false positive rate while keeping the effectiveness of identifying Sybil nodes with an acceptable tradeoffs [1].

System Model : Here assume that in the system there are n honest users representing real human beings, and each of them has exactly one honest identity, which is denoted as an honest node in the social network graph. It is assumed that a social network graph comprises multiple communities of different sizes. To verify assumption, conducted experiments on a 100,000-node sample graph from MySpace [9] by applying Louvain Method [10] for community detection. Result shows that these 100,000 nodes can be divided into 19 communities, with smallest size of 12 and largest size of 33,877, inter-connected by ten to hundreds of edges. This result validates the assumption and is also consistent with the observation made in previous work [10], [11].

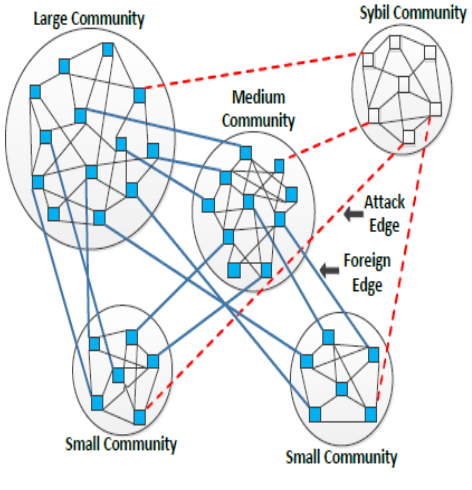

Figure 2. The Social Network Graph [1]

Fig. describes the social network topology wherein honest nodes compose multiple groups of different sizes, and those are inter-connected with each other and termed honest communities/regions. Correspondingly, community formed by Sybil nodes is termed Sybil community/region [9].

Categorize honest communities into three types according to their sizes: small community, medium community, and large community. If there exists an edge between two nodes located in different communities, we call it a foreign edge. Moreover, if one of the nodes connected by a foreign edge is a Sybil, we say this edge is an attack edge, through which the adversary may deceive other honest nodes.

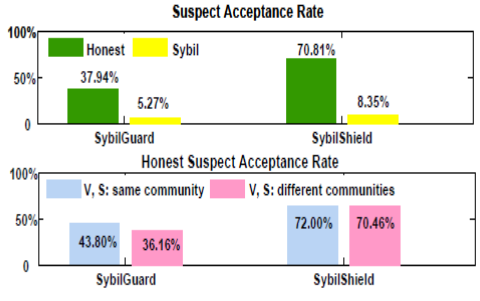

Figure 3. Honest & sybil suspects acceptance ratio for v & s from same/different communities[1].

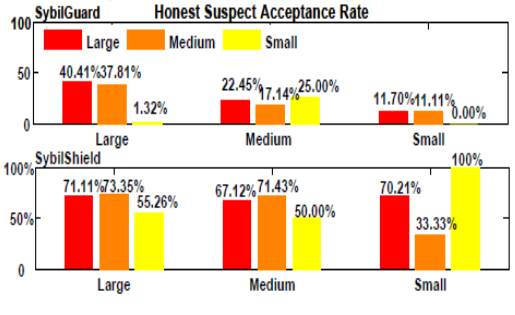

Figure 4.Honest & sybil suspects acceptance ratio for each type of community [1]

Lu Shi, Shucheng Yu et.al have compared SybilShield against SybilGuard [1]. As per their finding first half of Fig.3, the acceptance rate of honest suspects for SybilShield and SybilGuard is 70.81% and 37.94%.Therefore, the false positive rate is effectively reduced by 32.87%. Accuracy of identifying honest suspects in SybilShield is improved twice as much in SybilGuard because of the introduction of agents. In the other half of the same fig. whether in SybilShield or SybilGuard, the accuracy of identifying honest suspects is reduced by 1.54% and 7.64%.The honest suspects

acceptance rate is enhanced from 43.8% and 36.16% in SybilGuard to 72.00% and 70.46% in SybilShiled. Another Fig reveals the effect of community type on the honest suspect's acceptance rate in both SybilGuard and SybilShield. We can easily see that compared to SybilGuard, the overall acceptance rate in SybilShield nearly doubles, especially for honest suspects in medium and small communities [1].

3.3. SybilLimit

SybilLimit, a near-optimal defense against sybil attacks with the use of social networks. If it is compared to previous SybilGuard protocol that accepted $O(\sqrt{n}\log n)$ sybil nodes per attack edge, SybilLimit accepts only $O(logn)$ sybil nodes per attack edge. In addition, SybilLimit provides this guarantee even when the number of attack edges grows to $O(n/logn)$. SybilLimit's improvement derives from the combination of multiple novel techniques: 1) leveraging multiple independent instances of the random route protocol to perform many short random routes; 2) exploiting intersections on edges instead of nodes; 3) using the novel balance condition to deal with escaping tails of the verifier; and 4) using the novel benchmarking technique to safely estimate [4]. Finally, results on real-world social networks confirmed their fast-mixing property and therefore it has also validated the fundamental assumption behind SybilLimit's and SybilGuard's approach.

SybilLimit[4] presented a new protocol that leverages the same insight as SybilGuard but offers dramatically improved and near-optimal guarantees. The protocol's name is SybilLimit because: 1) it limits the number of sybil nodes accepted; and 2) it is near-optimal and thus pushes the approach to the limit. For any $g = o(n/\log n)$, SybilLimit can bound the number of accepted sybil nodes per attack edge within $O(\log n)$(see Table I). This is a $\theta(\sqrt{n})$ factor reduction from SybilGuard's $O(\sqrt{n}\log n)$guarantee. In their experiments on the million-node synthetic social network[4], Haifeng Yu, Phillip B. Gibbons et al. found that SybilLimit accepts on average around 10 sybil nodes per attack edge, that again leads to 200 times improvement over SybilGuard. That is with SybilLimit the adversary needs to establish almost 100 000 real-world social trust relations with honest users in order for the sybil nodes to outnumber honest nodes, as compared to 500 trust relations in SybilGuard. It has further proved that SybilLimit is at most a factor from optimal in the following sense: For any protocol based on the mixing time of a social network, there is a lower bound of $\Omega(1)$ on the number of sybil nodes accepted per attack edge. Finally, SybilLimit continues to provide the same guarantee even when g grows to $o(n/\log n)$, while SybilGuard's guarantee is voided once $g = \Omega(\sqrt{n}/\log n)$. Achieving these near-optimal improvements in SybilLimit is far from trivial and requires the combination of multiple novel techniques. SybilLimit achieves these improvements without compromising on other properties as compared to SybilGuard (e.g., guarantees on the fraction of honest nodes accepted).

Table 1. Number of sybil nodes accepted per attack edge (out of an unlimited number of sybil nodes),both asymptotically for n honest nodes and experimentally for a million honest nodes. Smaller is better.

Number of attack edges g (unknown to protocol)	**SybilGuard Accepts**	**SybilLimit accepts**
$o(\sqrt{n}/\log n)$	$O(\sqrt{n}\log n)$	$O(\log n)$
$\Omega(\sqrt{n}\log n) to\ o(\sqrt{n}/\log n)$	Unlimited	$O(\log n)$
Below ~ 15000	~ 2000	~10
Above ~ 15000 and below ~100100	Unlimited	~10

3.4. SybilDefender

SybilDefender, a scheme that leverages network topologies to defend against sybil attacks in large social networks. SybilDefender consists of a sybil identification algorithm and a sybil community detection algorithm. It also includes two approaches to limiting the number of attack edges in online social networks. Evaluation on two large-scale real-world social network samples shows that SybilDefender can correctly identify sybil nodes, even when the number of sybil nodes introduced by each attack edge approaches the theoretically detectable lower bound, and that it can effectively detect the Sybil community surrounding a sybil node with different sizes and structures [2].

SybilDefender is based on performing a limited number of random walks within the social graphs. This technique is really efficient and scalable to large social networks. Their experiments on two 3,000,000 node

real world social topologies show that SybilDefender outperforms the state of the art by more than 10 times in both accuracy and running time. The survey results of their Facebook application show that the assumption made by previous work that all the relationships in social networks are trusted does not apply to online social networks and that is why it is possible to limit the number of attack edges in online social networks by relationship rating [2].

3.5. SyMon

Sybil attack is one of the most challenging problems that plague current decentralized peer-to-peer systems. In short Sybil attack is the attack where a single malicious user creates multiple peer identities known as sybils. These sybils are then used to target honest and genuine peers and hence weaken the system. In this paper, a novel solution is proposed that enables all honest peers to protect themselves from sybils with high probability in large structured P2P systems. In proposed sybil defense system, every peer associated with another non-sybil peer called as SyMon. Then a given peer's SyMon is selected dynamically such that the chances of both of them being sybils are very low. The selected SyMon is delegated the responsibility of moderating the transactions involving the given peer and hence makes it almost impossible for sybils to compromise the system. It shows the effectiveness of proposed system in defending against Sybil attack both analytically and experimentally [5].

4. Conclusions

Sybil attacks are very critical for distributed decentralized systems like social network and threat is even serious as a lot of personal and sensitive information is shared across social networking sites. Many researchers have suggested techniques like SybilGuard, SybilShield, SybilLimit, SybilDefender, SyMon. There is still future scope to build up on this research to evolve better and stronger defense system against sybil attack. This paper studies all these current defense techniques. SybilGuard is a novel protocol for limiting the corruptive influences of sybil attacks and bounds the number of identities a malicious user can create. These recent techniques have been analyzed and compared. SybilShield is the first protocol that defends against Sybil attack using multi-community social network structure in real world. SybilLimit protocol leverages the same insight as SybilGuard, but offers dramatically improved and near-optimal guarantees. SybilDefender is a defense mechanism that leverages the network topologies to protect against sybil attacks in social networks and is efficient, scalable to large social networks, based on performing a limited number of random walks within the social graphs. SyMon better defense technique in large structured P2P systems where it associate every peer with another non-sybil peer known as SyMon, moderating the transactions involving the given peer and hence makes it almost impossible for sybils to compromise the system.

5. REFERENCES

[1] Lu Shi, Shucheng Yu, Wenjing Louy and Y. Thomas Hou "SybilShield: An Agent-Aided Social Network-Based Sybil Defense among Multiple Communities", IEEE Infocom 2013.

[2] Wei Wei, Fengyuan Xu, Chiu C. Tan, and Qun Li "SybilDefender: A Defense Mechanism for Sybil Attacks in Large Social Networks",IEEE Transactions on parallel and distributed systems, vol. 24, no. 12, December 2013

[3] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbon, Abraham D. Flaxman "SybilGuard: Defending Against Sybil Attacks via Social Networks" IEEE/ACM Transactions on networking, vol. 16, no. 3, June 2008

[4] Haifeng Yu, Phillip B. Gibbons, Member, IEEE, Michael Kaminsky, and Feng Xiao "SybilLimit: A Near-Optimal Social Network Defense Against Sybil Attacks" IEEE/ACM Transactions on networking, vol. 18, no. 3, June 2010

[5] Jyothi, B.S.; Dharanipragada, J. "SyMon: Defending large structured P2P systems against Sybil attack" IEEE 2009

[6] C. Lesniewski-Laas, M. F. Kaashoek. "Whanau: A sybilproof distributed hash table". In NSDI, San Jose, CA, 2010, USENIX Association.

[7] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig "The Sybil Attack in Sensor Networks: Analysis & Defenses" Information Processing in Sensor Networks, 2004.

[8] Wei Chang, Jie Wua "Survey of Sybil Attacks in Networks"

[9] Y.Y. Ahn, S. Han, H. Kwak, S. Moon, and H. Jeong, “Analysis of topological characteristics of huge online social networking services,” in WWW ’07: Proceedings of the 16th international conference on World Wide Web. New York, NY, USA: ACM, 2007, pp. 835–844.

[10] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre, “Fast unfolding of communities in large networks,” Journal of Statistical Mechanics: Theory and Experiment, vol. 2008, October 2008.

[11] M. E. J. Newman, “Modularity and community structure in networks,” Proceedings of the National Academy of Sciences, vol. 103, no. 23, pp. 8577–8582, 2006