ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

A Survey of Techniques to Defend Against Sybil Attacks in Social Networks

Rakesh G.V [1], Shanta Rangaswamy [2], Vinay Hegde [3], Shoba G [4]

IV sem M.Tech (CNE), Dept of CSE, RVCE , Bangalore, India[1]

Assistant Professor, Dept of CSE, RVCE , Bangalore, India[2]

Assistant Professor, Dept of CSE, RVCE , Bangalore, India[3]

Head of the Department, Dept of CSE, RVCE , Bangalore, India[4]

Abstract: Most peer-to-peer systems are vulnerable to Sybil attacks. The Sybil attack is an attack where in an adversary creates multiple Duplicate or False identities to compromise the running of the system. By including false information by the Duplicated entities, an adversary can mislead a system into making decisions benefiting . For example, in a distributed review system, an adversary can easily change the overall review of an option by providing plenty of false praise, the option through these fake identities. Defending against Sybil attacks is quite challenging. In this paper, we summarize the existing Sybil defense techniques, we first group the Sybil defense methods, mainly according to their type, and then divide the methods by their approaches**.**

Keywords: peer-to-peer systems, Security, Sybil attack, Defense

I. INTRODUCTION

A Sybil attack [1] is one in which a malicious node on a network illegitimately claims to be several different nodes simultaneously. Many distributed applications and everyday services assume each participating entity controls exactly one identity. When this assumption is un verifiable the service is subject to attack. In a large-scale peer-to-peer system, a direct connection between each pair of nodes is impossible, therefore, the nodes which are participating usually create networks, and a message is transmitted from one node to another via the relay operations of multiple intermediary nodes. In this paper, we investigate the Sybil attack, a dangerous attack in distributed peer-to-peer networks.

Almost distributed peer-to-peer systems are based on a common assumption that each participating entity controls exactly one identity. However, whenever the assumption cannot be fulfilled, the system lead to Sybil attacks.

In a Sybil attack, an adversary creates a large number of false/fake/Duplicate identities (Sybil identities), and since all Sybil identities are controlled by the adversary, It can maliciously introduce a considerable number of false opinions into the system, and convert it, by making decisions benefiting system itself. Let's consider example comes from a Facebook voting application. If an attacker maliciously creates many identities, it can easily change the overall popularity of an option by providing plenty of false praise, of the option through Sybil ids. Since the false opinions of the Sybil's may essentially change the final decision of any distributed system.

II. DIFFERENT TYPES OF SYBIL ATTACKS

There are various defected applications of Sybil attacks in different areas such as those including, but not limited to, the variations enlisted below.

1. Routing in a Distributed Peer-to-peer System

To improve the performance wireless networks usually adopt a multi-path routing technique. Instead of using a single routing path, multi-path routing has multiple paths throughout a network. The computed multi-paths may or may not be overlapped. This technique provides better load balancing within the nodes and performance than traditional routing methods. However, in wireless sensor networks, Sybil attacks can easily invalidate the technique ,a computed multi-path routing, which consists of multiple disjoint paths, could in fact only go through the same defected node, which holds several Sybil identities.

Other wireless routing types, such as the decentralized object location and routing (DOLR) algorithm, and the geographic routing algorithm, are also easily affected by Sybil attacks. In distributed networks, nodes communicate with each other by relaying messages from one node to another node and the quality of the selected paths directly influences the fault tolerance of a network system. In some cases, Sybil attack may even move from one part of a network from the other part.

2. Distributed Storage Applications in Peer-to-peer Systems

Distributed storage systems adopt duplication and splitting mechanisms, and usually the mapping from data to the corresponding stored nodes is performed by using hash functions distributed hash tables. By considering the system stability and easy accessing, the mapping function must be in the form of one-to-many.

If the attacker is an insider, he can manipulate the values of his Sybil identities such that all the replicated data may actually be stored on the same malicious node, although the data seems to be stored at different nodes outwardly.

Without multiple copies of data, the attacker can easily cause many followed attacks without being identified. For example, he can change some data. Because he holds all of the data copies, nobody can detect the modification of the data.

3. Distributed Voting Applications in Peer-to-peer Systems

Any distributed voting aggregation system is vulnerable to Sybil attacks. Usually, a distributed voting system consists of a collection of identities which vote for different entities. Most of the voting systems assume that each user has one identity, and by using that identity he can provide only one vote. Based on this constraints, if attacks have multiple identities, then he can have multiple votes. The vote can be in any type, from the simplest case, where each vote represents a positive or a negative opinion, to more cases, the value of a vote can range within a given set of values. To rank objects, a ranking mechanism typically collects (or aggregates) the votes from distributed participants and further combines the votes in a certain method, such as the majority rule. By Sybil attack, the real users' major decision can be out-voted by the attacker: since the attacker can easily create many duplicate fake identities, the wrong opinions can be introduced into the system by these fake identities. Here, we need to prove that, although the Sybil nodes may be held by different attackers for the easy understanding the researchers always assume that the Sybil identities are kept by a single entity. Because of this assumption it will not influence the effects of the attacks, and will also not affect the results of different approaches.

The example of Flipkart's user feedback system in the introduction is essentially an grouping voting system,

Since the reputation of each merchant is determined by the votes from customers. However, we also have to mention that the Flipkart voting system is a centralized system, where all of the voting processes are controlled by a central server. However, generally, an aggregating voting system can also be a distributed system, each node can provide a vote, and the range of votes' values may different.

4. Vehicular Ad hoc Networks (VANETs)

A Vehicular Ad-Hoc Network is a advanced technology it uses moving cars as nodes to create a special mobile network..In VANETs, each car on a road can communicate by signals with roadside base stations or other cars. However, this type of network is easily vulnerable to Sybil attack. For example, a driver may launch a Sybil attack by misleading that many vehicles are traveling nearby. If this is the case, other cars may wrongly believe that there is a traffic jam on the corresponding road, and therefore chooses an alternative road. The selfish driver will enjoy better traffic, with others must face heavy traffic. Moreover, the Sybil attacks can also cause serious safety threats, a malicious driver may drop the wrong warning messages. In VANETs, when a accident happens or speed gradually reduces, a warning message for slowing-speed will be generated, and is further passed to the near by vehicles in that road, one-by-one. By providing many fake identities, the warning messages may all be transmitted to the malicious driver's car. If he drops these messages, other following cars will be in danger.

.

5.Data Aggregation in peer-to-peer Applications

Sensor network readings are computed by query protocols [2] in a network rather than returning the reading of each individual sensor. This is done to conserve energy. Sybil identities may be able to report incorrect sensor readings thereby influencing the overall computed aggregate. A malicious user may be able to significantly alter the aggregate with enough identities.

6. Sock puppets in Online review Forums

In online review forums, in order to cheat people on the Internet, for example, to believe that a product is a good buy, a usual plan is to use different duplicate online identities pretending to be different people. This is done to increase the value of for the product [3]. In the same forum, different online entities which belong to the same person are referred as 'sock puppets.' Note that sock puppet does not belong to Sybil attack, since online discussion forums are not peer-to-peer systems. However, because sock puppets have several features similar to Sybil attacks, we want to mention them. Both attacks are based on the creating of multiple identities belonging to the same person. Second, their success is related to the same assumption that each user is associated with one, and only one, identity. Third, they all break the reputation mechanism behind a given system. Last, for some distributed network systems, such as mobile social networks, there are social features associated with each identity, this also applies to an online discussion forum. Due to these similarities, the solution to one attack may help the to identify the other.

III. METHODS PROPOSED TO DEFEND SYBIL ATTACKS

A number of approaches for various combinations of environments and attacks have been proposed. Some methods mitigate the threat level of these attacks in a system to a satisfactory minimum without incurring an appreciable performance overhead .There are many methods proposed to control the Sybil attacks are as follows.

1. Trusted Certification

Sybil attacks can be avoided by using trusted certification. In this method central authority, they can verify the validity of each user, and further issues a certification for the honest one. In real world, such certification can be a special hardware device [4] or a digital number [5], [6].Before a participant joins a peer-to-peer system, provides votes, and to obtains services from the system, his identity must first be verified. For example, when we are applying for a bank atm card, we need to give our social security number for verification.

Centralized trusted certification methods are often implemented by asymmetric (such as public/private keys) Cryptography.

They assumed that each node shares a unique symmetric key with a trusted centralized base station. After checking the validity of each other ,a pair of nodes can establish a shared key. During data transmission between adjacent nodes, they can use the key for mutual authentication and validation, and can also encrypt the data.

Problems with Trusted Certifications

The problems associated with the central authority-based methods, as follows:

a) Single point of attack. In these schemes, the central authority can easily become a target.

b) Performance bottleneck. If many users access a central authority simultaneously, the central authority may fail.

c) Communication cost. In this type of method, the authority should be required during the data transmission.

2. Registration Fee: Unlike the trusted certification-based approaches, some other papers [7]–[8] add an economical “fee” with each certification. They judge that the attackers cannot easily join and affect a peer-to-peer system unless they spend a lot of money. Indeed, they intend to build a system letting the cost of an attack outweigh the benefits of the attack.

3. Resource Testing:

Resource Testing is the most commonly implemented solution to averting Sybil attacks. The basic principle is that the quantum of computing resources of each entity on the network is limited. Usually, each user can have only one identity, and each identity should work on a single machine.

However, when Sybil attacks are started, the Sybil identities work on a single system. When we give some constraints like time or resource consuming tasks to a group of identities, if they can complete the work within a threshold, then it is most possible that they are honest nodes. otherwise, it can contain some Sybil nodes. In general, the goal of resource testing [9]–[10] is to determine whether the selected identities have a reasonable amount of resources.

The tests, include: computing ability, storage ability, and checking testing is not an efficient.

4. System Specific Features- Location / Position Verification

This solution is specific to Wireless ad hoc Networks.

Consider that there are channel conflicts during the communication of honest users, while Sybil nodes do not have real data transmission. Paper [11] proposed aSybil detection method by monitoring the neighbors’ channel conflict rate. They assume that there is a central Authority that records the rate of each identity. Whenever a channel change happens, some nodes should send that event to the central authority. If some nodes have an low rate, then the central authority will decide them as Sybil identities.

5.Social Network Based Techniques to Defend Sybil Attacks.

Here the Sybil attacks detected based on a unique structure: although attackers can create plenty of Sybil identities, and further establish several links among them; the total number of links between the Sybil and the honest users is limited, since the trust relationship on a social network is built based on the trust relationship among real people.

5.*1 Sybil Guard and Sybil Limit*

Sybil Guard [12], and Sybil Limit [13] are two famous Sybil defenses that use social networks. we will only introduce Sybil Guard. Sybil Guard defines two terms,

1 a trusted path, 2. A trusted node.There is similarly, for breaking the symmetric data constriction, Sybil Guard also assumes that there is a known trusted node. From this trusted node, there are ‘K’ random paths with a fixed length . For the ease of description, we call these paths verifiers. From a suspect node, Sybil Guard also sends ‘k’ random paths. If a path encounters a verifier once, then we call the path ‘been verified once. If a path has been Verified ‘S’ times, then the path is a trusted path. When the most of the paths of a suspect node are trusted paths, the suspect node will be treated as a trusted node; otherwise the node is a Sybil. Sybil Guard suffers from high false negatives, as each attack edge may introduce $O(\sqrt{n} \log n)$ Sybil nodes without being detected. The advanced version of Sybil Guard, Sybil Limit, reduces this value to $O(\log n)$, to detect the Sybil region with Sybil Guard or Sybil Limit, all the suspect nodes in the social graph need to be tested.

5.2 Sybil Infer

Sybil Infer [14], a centralized Sybil defense algorithm, leverages a Bayesian inference approach that assigns a Sybil probability, indicating the degree of certainty, to each node in the network. It achieves low false negatives at the cost of high computation overhead. The overall time complexity of Sybil Infer is O(|V |2 log |V |), where V is the set of vertices in the social graph. In the evaluation Sybil Infer handled networks with up to 30K nodes, which is much smaller than the size of regular online social networks.

5.3 Gate Keeper

Gate keeper[15], a decentralized protocol that performs Sybil-resilient node admission control mainly based on a social network. Gatekeeper can admit most honest nodes while limiting the number of Sybil’s admitted per attack edge toO(log k), where k is the number of attack edges. Gate Keeper scheme that heavily relies on the assumption that the social networks are random expander. This is a strong assumption which has not been validated by previous research. Our evaluation shows that GateKeeper suffers from high false positive and negative rates and cannot effectively identify Sybil nodes on the real-world asymmetric social topologies.

5.4Sybil Defender

Sybil Defender[16], a Sybil defense mechanism that leverages the network topologies to defend against Sybil attacks in social networks. Based on performing a minimum number of random walks within the social graphs, Sybil Defender is most efficient and it is scalable to large social networks. Sybil Defender can effectively identify the Sybil nodes and detect the Sybil community around a Sybil identity, even when the number of Sybil nodes introduced by each attack edge is close to the theoretically detectable lower bound. Sybil Defender consists of two components: a Sybil node identification algorithm, a Sybil group around that Sybil node detection algorithm.

IV. CONCLUSION

However, most of the peer-to-peer systems are vulnerable to Sybil attacks. In this paper, we have discussed the important kinds of Sybil attacks that can be applied on various application domains. We have also listed important techniques that have been proposed to defend the Sybil attacks.

REFERENCES

[1] J. R. Douceur, The Sybil attack, In Proceedings for the First International Workshop on Peer-to-Peer Systems (IPTPS'02), ser. LNCS, vol. 2429. Cambridge, MA, USA: Springer, Mar. 2002, pp. 251–260.

[2] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, TAG: a tiny aggregation service for ad hoc sensor networks, ACM SIGOPS Operating Systems Review - OSDI '02: Proceedings of the 5th symposium on Operating systems design and implementation Volume 36 Issue SI, Winter 2002 Pages 131-146

[3] X. Zheng, Y. Lai, K. Chow, L. Hui, and S. Yiu, "Sockpuppet detection in online discussion forums," in Proc. of IEEE IIH-MSP, 2011

[4] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," in Proc. of ACM IPSN, 2004 pp. 259–268.

[5] J. Ledlie and M. Seltzer, "Distributed, secure load balancing with skew, heterogeneity and churn," in Proc. of IEEE INFOCOM, vol. 2, 2005, pp. 1419–1430.

[6] G. Mathur, V. Padmanabhan, and D. Simon, "Securing routing in open networks using secure traceroute," in Technical report MSR-TR- 2004-66, Microsoft Research, 2004.

[7] B. Awerbuch and C. Scheideler, "Group spreading: a protocol for provably secure distributed name service," in Automata, Languages and Programming. Springer, 2004, pp. 183–195.

[8] Y. Reddy, "A game theory approach to detect malicious nodes in wireless sensor networks," in Proc. of IEEE SENSORCOMM, 2009, pp. 462–468.

[9] P.W. L. Fong. Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems. In IEEE Symposium on Security & Privacy, 2011 pp. 263-278.

[10] B. Carminati and E. Ferrari, Enforcing relationships privacy through collaborative access control in web-based social networks, In Proceedings of the 5th International Conference on Collaborative Computing: Networking, Applications and Work sharing CollaborateCom'09), Washington DC, USA, Nov. 2009 pp. 1-9, 2009

[11] C. ZHENG and D. S. GILBERT, "Thwarting sybil attacks and malicious disruption in wireless networks," http://www.comp.nus.edu.sg/ zheng-10/talk/grp-2012-09-14-paper-v3.pdf.

[12] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in Proc. of ACM SIGCOMM, vol. 36, no. 4, 2006, pp. 267–278

[13] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: a near-optimal social network defense against sybil attacks," in Proc. of IEEE Symposium on Security and Privacy, 2008, pp. 3–17.

[14] G. Danezis and P. Mit. Sybilinfer: Detecting sybil nodes using social networks. In NDSS, 2009.

[15] N. Tran, J. Li, L. Subramanian, and S. S.M. Chow. Optimal sybilresilientnode admission control. In IEEE INFOCOM, 2011.

[16] SybilDefender: Defend Against Sybil Attacks in Large Social Networks Wei Wei∗, Fengyuan Xu∗, Chiu C. Tan†, Qun Li The College of William and Mary, †Temple University