International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730

Sybil Attack in Peer-to-Peer Network

ChinkyAggarwal,Email-rashigarg04@gmail.com
SRCEM, Palwal, Haryana

Abstract—Any decentralized distributed network is particularly vulnerable to the Sybil attack wherein a malicious node, called Sybil nodes tries to disrupt the proper functioning of the network. Such attacks may cause damage on a fairly large scale especially since they are difficult to detect and there has been no universally accepted scheme to counter them as yet.
In this paper, we survey the impact of the Sybil attack , an attack against identity in which an individual entity masquerades as multiple simultaneous identities. The Sybil attack is a fundamental problem in many systems, and it has so far resisted a universally applicable solution. Many distributed applications and everyday services assume each participating entity controls exactly one identity. When this assumption is unverifiable or unmet, the service is subject to attack and the results of the application are questionable if not incorrect. A concrete example of this would be an online voting system where one person can vote using many online identities. Notably, this problem is currently only solved if a central authority, such as the administrator of a certificate authority, can guarantee that each person has a single identity represented by one key; in practice, this is very difficult to ensure on a large scale and would require costly manual attention.

KEYWORDS-Peer to Peer(P2P),Certifying Authority
(CA), ”servant" (SERver+cliENT).Received Signal Strength Indicator(RSSI),IdentityDistributionScheme(IDS),NETWORK ATTACK

I. INTRODUCTION

Peer-to-Peer systems offer an alternative to traditional client-server systems for some application domains. P2P network is a distributed network composed of a large number of distributed, heterogeneous, autonomous, and highly dynamic peers in which participants share a part of their own resources such as processing power, storage capacity, software, and files contents. The participants in the P2P network can act as a server and a client at the same time. They are accessible by other nodes directly, without passing intermediary entities. The P2P models can be pure or hybrid. In pure P2P any single, arbitrary chosen terminal entity can be removed from the network without having the network suffering any loss of network service. Hybrid P2P allows the existence of central entities in its network to provide parts of the offered network services.
There are several concepts underlying p2p systems: sharing resources, decentralization and self organization. Resource sharing implies that applications cannot be set up by a single node. Shared resources can be physical re-sources such as disk space, CPU or network bandwidth, as well as, logical resources

such as services or different forms of knowledge. Decentralization is an immediate consequence of sharing of resources. Decentralization is in particular interesting in order to avoid single point of failures and bottlenecks. When a p2p system becomes fully decentralized then there exists no longer a node that can centrally coordinate its activities or a database to store global information about the system centrally. Therefore nodes have to self-organize themselves, based on whatever local information is available and interacting with locally reachable nodes (neighbors). The global behavior then emerges as the result of all the local behaviors that occur.
There are several concepts underlying p2p systems: sharing resources, decentralization and self organization.
Sybil attack has appeared in many forms in both academic work and in the real world. It is a severe and pervasive problem in many areas. For example, it is possible to rig Internet polls by using multiple IP addresses to submit votes , to gain advantage in any results of a chain letter , and is a well-known and potentially major problem in real-world elections. A Sybil attack is also used by companies that increase the Google Page Rank rating of the pages of their customers, has been used to link particular search terms to unexpected results for political commentary. Reputation systems are a common target for Sybil attacks including real-world systems like eBay.
Spammers can use this attack to gain access to multiple accounts on free email systems. Peer-to-peer computing systems which use voting to verify correct answers, such as SETI@home, are also susceptible to accepting false solutions from a Sybil attacker. Ad hoc mobile network routing can be manipulated when a Sybil attacker appears to be many different mobile nodes at once.In systems that provide anonymity between peers, such as Tor, the Sybil attack is generally capable of revealing the initiator of a connection and there is no defense against this attack. It also allows free riding in services in cooperative file storage systems such as Pastiche.

II. SPECIFIC TYPES OF SYBIL ATTACKS

There are numerous malicious applications of Sybil attacks in different environments such as those including, but not limited to, the variations enlisted below.

A. Routing

Sybil attacks can disrupt routing protocols in ad hoc networks, especially the multicast routing mechanism.
Separate paths that initially seem disjoint may pass through the Sybil nodes of a single attacker. Another vulnerable concept is Geographical routing where malicious nodes may appear at more than one place at a time.
An attack in an ad hoc network and thus the availability of fake identities may further lead to a large scale attack such as distributed DoS, in addition to the inherently insecure
routing protocols in such networks named as ”servant” (SERver+cliENT), the term servent represents the capability of the nodes of a peer-to-peer net-work of acting at the same time as server as well as a client.

B. Tampering with Voting and Reputation Systems

In case of any environment where there is a voting scheme in place for purposes such as reporting and identifying node misbehavior in the system, updating reputation scores and so on, a Sybil attack may be particularly dangerous. As an example, an attacker may create enough malicious identities to repeatedly report and subsequently remove legitimate nodes from the network. Alternatively, these malicious nodes can protect themselves from ever being removed as they are in collusion.

C. Distributed Storage

File storage systems in peer-to-peer and wireless sensor networks can be compromised by the Sybil attack. This is achieved by defeating the fragmentation and replication processes in the file system. A system can be tricked into storing data into the multiple Sybil identities of the same node on the network.

D. Data Aggregation

Sensor network readings are computed by query protocols 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.

III. METHODS PROPOSED TO COUNTER SYBIL ATTACKS

Though there is no general, universally-accepted solution to the Sybil attack, 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. We must note that although they will not completely eliminate the possibility of the attack occurring, they are more than worthy of consideration.
Notable techniques to counter Sybil attacks are as under.

A. Trusted Certification

Certification is by far the most frequently cited solution to defeating Sybil attacks. It involves the presence of a trusted certifying authority (CA) that validates the one is to one
correspondence between an entity on the network and its associated identity. This centralized CA thus eliminates the
problem of establishing a trust relationship between two communicating nodes. Douceur has proven that such kind of certification is the only method that may potentially
eliminate Sybil attacks completely . Although this approach intuitively seems like the ideal method to tackle these attacks, there are a number of implementation issues specifically about how the CA shall establish the entity-identity mapping. In real-world applications this may incur an appreciable performance cost particularly if performed manually on large scale systems.

B. 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. A verifier then checks whether each identity has as many resources as the single physical device it is associated with. Any discrepancy indicates the possibility of a compromised node. Storage, computation and communication were initially proposed as resources. However, for a system such as a wireless sensor network, an attacker might have storage and computation resources in large capacities compared to resource-starved sensor nodes. Alternatively,

verification messages for verifying communication resources might flood the entire system itself. Hence, all three are inadequate choices for sensor networks.

Radio resource testing, proposed by Newsome et al. in [6], is an extension of the resource testing verification method for wireless sensor networks. The key assumptions of this approach are that any physical device has only one radio and that this radio is incapable of transmitting and receiving messages on more than one channel at any given time.

Resource tests have been suggested by many as a minimal defense against Sybil attacks where the goal is to reduce their risk substantially rather than to eliminate it altogether.

C. Identity Distribution Scheme

It is intended to prevent a node from obtaining a huge number of fake identities. This scheme is based on invitations and distribution of a set of identities (which can be used by a node for inviting others) to each node in the network.

For obtaining an identity on the network or, for a node to become a part of the network, it has to be invited by an existing member. When a node joins the network, a set of identities are assigned to each node by the parent node for inviting others. So there should be a control on the count of identities offered to each node, otherwise a malicious node
could create an unlimited number of sybil identities either directly by inviting them or indirectly by inviting some sybils which in turn invite other sybils.The proposed scheme intends to prevent an attacker from creating an unlimited number of sybil nodes, even though a genuine node can invite new nodes. Thus, the growth of the network is on the basis of how identities are assigned to each node and how they use it.

The proposed scheme can be used by P2P service providers
for node admission, by limiting the entry of sybil identities into the system. Initially few pre-trusted peers with sufficient CPU, memory and network bandwidth are assigned as super nodes by the service provider. So we consider a P2P network where nodes can be categorized into two: peers/regular clients and super nodes/super peers. The super nodes and peers are interconnected.A group of peers will be monitored by a super node and every super node is connected to at least another super node. The network topology is shown in Figure 1. For a node to join the network, it must be invited by some member (it can be a super node or peer) in the network. Every super peer is assumed to have a set of invitations/identities (say N). When a node invites another
node, the former is called parent and the latter is called the child. When a node accepts the invitation from another node, the parent assigns a unique identifier and a set of identities (for inviting others) to its child. Here the issue is what fraction of identities from parent is to be assigned to the child (see Section 3.1). Each node (either super node or peer) in the network is assumed to have
the following parameters:

- A unique identifier
- Identifier of parent
- Identifier of the super node under which it comes
- A public key- private key pair
- Count of used Invitation
- Range of invitations it can use, indicating lower limit and upper limit of node numbers (here invitations correspond to set of identities.)
- A Timestamp assigned to each child by the parent when a set of identities are assigned to it.

The first three parameters are identical in case of a super node (identifier of the super node). The unique identifier of a peer is composed of two parts. The first part indicating the super node under which it comes and second part is the node number under the corresponding super node. Each node will store the unique identifiers of nodes it has directly invited, along with their assigned range of invitations and timestamp showing when it has assigned those invitations. In addition to these, if the node is a super node it will maintain a list of all nodes under it, either directly or indirectly invited.

D. RSSI-based scheme

Demirbas and Song introduce a method for Sybil detection
based on the Received Signal Strength Indicator (RSSI) of
messages. The cooperation of one additional node (and)
hence one message communication) is required for the
proper functioning of this protocol. A localisation algorithm is used in this scheme Sybil attacks can be detected with a completeness of 100% with few false positive alerts. Despite the fact that RSSI is unreliable and that transmissions via radio are non-isotropic, the use of ratios of RSSIs from multiple receivers solves this problem.

IV. CONCLUSION

This paper proposes a simple mechanism for sybil resistant node admission in P2P networks. Using this scheme the sybil behavior of a node can be identified, and those suspected as sybils are limited from inviting others. Moreover nodes may contact one another for file sharing and super nodes calculate rank matrix and uses these values also for assignment of new identities. Although false positives and false negatives may occur in the labeling process, we have to minimize it as far possible, to improve the efficiency of the algorithm. In future, the efficiency of this algorithm can be increased by considering more parameters for labeling a node as sybil or genuine.

REFERENCES:

[1] Ratnasamy, S., Francis, P., Handley, M., Karp, R., and Shenker: A scalable content-addressable network. In Proceedings of ACM SIGCOMM San Diego, California, Aug. 2001.
[2] I. Stoica, R. Morris et al., "Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications," IEEE/ACM Trans. Net., vol. 11, no. 1, 2003, pp. 17–32.
[3] A. Rowstron and P. Druschel, "Pastry: Scalable, Distributed Object Location and Routing for Large-scale Peer-to-peer Systems," Proc. Middleware, 2001.
[4] B. Y. Zhao et al., "Tapestry: A Resilient Global-Scale Overlay for Service Deployment," IEEE JSAC, vol. 22, no. 1, Jan. 2004, pp. 41- 53.
[5] P. Baecher, M. Koetter, T. Holz, F. Freiling, and M. Dornseif. The nepenthes platform: An efficient approach to collect malware. In Proceedings of 9th International Symposium On Recent Advances in Intrusion Detection (RAID'06), 2006.
[6] J.Douceur: The Sybil Attack. Proceedings of the First International Workshop on Peer-to-peer Systems. Springer, March 2002.
[7] J. Ledlie and M. Seltzer. Distributed, secure load balancing with skew, heterogeneity, and churn. In Proc. IEEE INFOCOM, Mar. 2005.
[8] Brian Neil Levine, Clay Shields, and N. Boris Margolin, "A Survey of Solutions to the Sybil Attack," Tech report 2006-052, University of Massachusetts Amherst, Amherst, MA, October 2006
[9] N. Borisov. Computational puzzles as sybil defenses. In Proceedings of the 6th IEEE International Conference on Peer-to-Peer Computing (P2P), volume 0, pages 171–176. IEEE Computer Society, 2006.
[10] P. Druschel and A. I. T. Rowstron. PAST: A large-scale, persistent peer-to-peer storage utility. In Proceedings of the 8th IEEE Workshop on Hot Topics in Operating Systems. IEEE Computer Society, 2001.
[11] B. Awerbuch and C. Scheideler. Group Spreading: A Protocol for Provably Secure Distributed Name Service. In Proc. Automata, Languages and Programming (ICALP), pages 183–195, 2004.
[12] H. Rowaihy, W. Enck, P. McDaniel, and T. L. Porta. Limiting sybil attacks in structured P2P networks. In INFOCOM, pages 2596–2600. IEEE, 2007