Detection of Sybil Attacks in Structured P2P Overlay Network

Abstract

The Sybil attack in computer security is an attack where in a reputation system is subverted by forging identities in peer-to-peer networks. The name was suggested in or before 2002 by Brian Zill at Microsoft Research. In a Sybil attack the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically. Main motto is to secure the Peer to Peer network (P2P) by Sybil attackers. Considering more parameter for labeling a node ‘genuine’ or ‘Sybil’. Our system has two server one is main server and another is trusted server. Trusted server is act as a centralized server so it has the complete list of members with their details. So when the new member is added to the network, trusted server take the identity check test with its database by checking the new member details with the complete database. If
it found common parameters then it label that member as Sybil otherwise genuine.

References


Index Terms

Computer Science

Networks

Keywords

Sybil Attacks, P2P Overlay Network, Server, Dot Net.