Topic 6: Security in Peer-to-Peer Networks

1 Guidelines

For P2P systems to be widely accepted and adopted, it must be secure. Unfortunately, securing applications in a P2P environment is much more challenging than the already hard problem of securing client-server or traditional distritbuted applications. This follows from the openness and autonomous nature of a P2P network. For example, as nodes can join and leave the network, this could turn out to be a potential (denial-of-service) threat that can disrupt the operations of the system. As another example, given that a (malicious) node may change its identity whenever it rejoins the network, it becomes more difficult to trust a newly joined node. Yet another example of security threat is that (malicious) nodes may not be operating according to the prescribed protocols - a node may not route requests, another may not store data, yet another may not serve requests even if it has the data, etc. In this topic, you should endeavor to survey some of the works in the literature that attempt to address some of the security issues mentioned above. Your focus should be on (a) Routing attacks; (b) Storage and retrieval attacks; (c) Denial-of-service attacks; (d) Verification of data and computation; (e) Free riding; (f) Privacy and anonymity, and (g) PKI-based security.