52524 Asia Samreen

40. Trust Management for P2P Networks

ABSTRACT

Peer-to-Peer networks are very popular these days due to their use in data and resource sharing. Trust and reputation of a peer not only make it easy to take a decision to ask for resource from the trustworthy node but also provide a way to punish evil peers for malicious act. Incentive mechanism provokes a peer to share resource and discourage the well known free riding. In this thesis we studied various proposed schemes regarding P2P networks and discuss some open issues about security which are also helpful for the future research work as well as we have provided solution of some problems such as to detect malicious peers, false rating problem and sudden change in the behavior of peers that are helpful in designing a novel and robust frame work for trust and reputation based incentive mechanism.

The basic idea is how to prevent the system from misbehavior of peers and how to detect them with the condition that system should not be crashed even in the presence of malicious peers.

Distributed environments such as P2P systems and Ad hoc networks, aim to enable a large-scale cooperation for resource sharing framework. Secure transactions along with ID based authentication are the challenging issues for such environments. We studied the role of Threshold cryptography in securing such systems; it distributes the key or provides sharing of a key by multiple individuals called shareholders engaged in encryption, decryption and signing.

The proposed Trust Framework RepIn (Reputation and Incentive) is based on Threshold cryptosystems for security purposes, a recommendation reputation technique to collect feedbacks for the acquired services and an incentive mechanism to attract and convince peers to be the honest and provide a balance in resource sharing so that no user try to free ride on other

resources. The major task is to separate honest peers from those who intend to do wrong and those that have already shown some misbehavior. This approach uses the algorithm of peer categorization, based on peer's credibility that, further, depends upon peer's trust value or reputation and peer's credit that peer earns as virtual money if offers any resource and pays if consumes resources.

The solution is feasible for especially cluster-based systems because of Super-peer based design. A Super-peer is one that responsible to send, receive and execute queries and to provide storage facilities. Furthermore, they take advantage of the heterogeneity of capabilities (e.g., bandwidth, processing power) across peers, which recent studies have shown to be enormous to run a huge system. However these systems are vulnerable to various types of threats such as stealth of identity known as masquerading attack, joint conspiracy or collusion and to consume more resources with zero or less contribution, which is well known as free riding. In this thesis we present a novel and efficient trust framework to counteract all these attacks. A survey has also been taken to reveal other hidden attacks and a small description of solutions is also a part of this thesis. We have provided a security analysis based on assumptions from the area of Cryptography and experimental results are also concluded based on mathematical formulation. A number of experiments have been made for the different scenarios to detect dishonest peers. Our proposed model is designed for the environment where sub-divisions of domain exist consisting of local entities, global entities and super entities. We have provided anonymity using distributed decryption key and our model builds dynamic trust, computing reputation combined with incentive to choose service provider. This model separates out suspecious peer from good honest peers ,however only a suspecious peer can improve reputation and credit while a bad peer will ultimately leave the system