Abstract of the Dissertation

**Combating Sybil attacks in cooperative systems**

by

Nguyen Tran

New York University

Professor Jinyang Li, Advisor

_Cooperative systems_ are ubiquitous nowadays. In a cooperative system, end users contribute resource to run the service instead of only receiving the service passively from the system. For example, users upload and comment pictures and videos on Flicker and YouTube, users submit and vote on news articles on Digg. As another example, users in BitTorrent contribute bandwidth and storage to help each other download content. As long as users behave as expected, these systems benefit immensely from user contribution. In fact, five out of ten most popular websites are operating in this cooperative fashion (Facebook, YouTube, Blogger, Twitter, Wikipedia).

A robust cooperative system cannot blindly trust that its users will truthfully participate in the system. Malicious users seek to exploit the systems for profit. Selfish users consume but avoid to contribute resource. The ultimate way to disrupt security and incentive mechanisms of cooperative systems is using Sybil attacks, in which the adversary creates many Sybil identities (fake identities) and use them to disrupt the systems’ normal operation. No security and incentive mechanism works correctly if the systems do not have a robust identity management that can defend against Sybil attacks.
This thesis provides robust identity management schemes which are resilient to the Sybil attack, and use them to secure and incentivize user contribution in several example cooperative systems. The main theme of this work is to leverage the social network among users in designing secure and incentive-compatible cooperative systems. First, we develop a distributed admission control protocol, Gatekeeper, that leverages social network to admit most honest user identities and only few Sybil identities into the systems. Gatekeeper can be used as a robust identity management for both centralized and decentralized cooperative systems. Second, we provide a vote aggregation system for content voting systems, SumUp, that can prevent an adversary from casting many bogus votes for a piece of content using the Sybil attack. Finally, we provide a robust reputation system, Credo, that can be used to incentivize bandwidth contribution in peer-to-peer content distribution networks. Credo reputation can capture user contribution, and is resilient to both Sybil and collusion attacks.