Decoupling Service and Feedback Trust in a P2P Reputation System

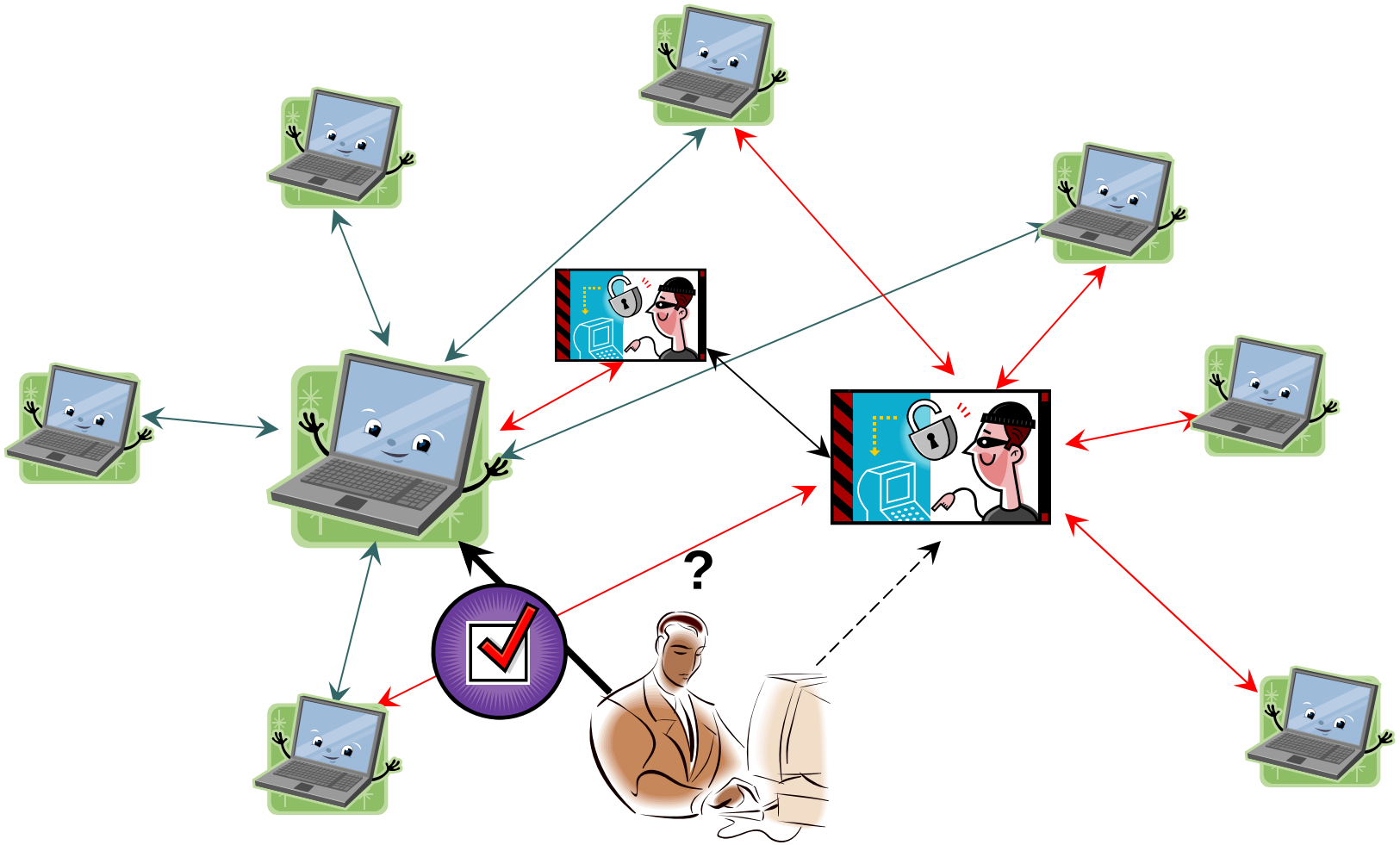
Gayatri Swamynathan Ben Y. Zhao Kevin C. Almeroth
Department of Computer Science
UC – Santa Barbara

AEPP 2005, Nanjing China

Security Challenges in P2P Networks

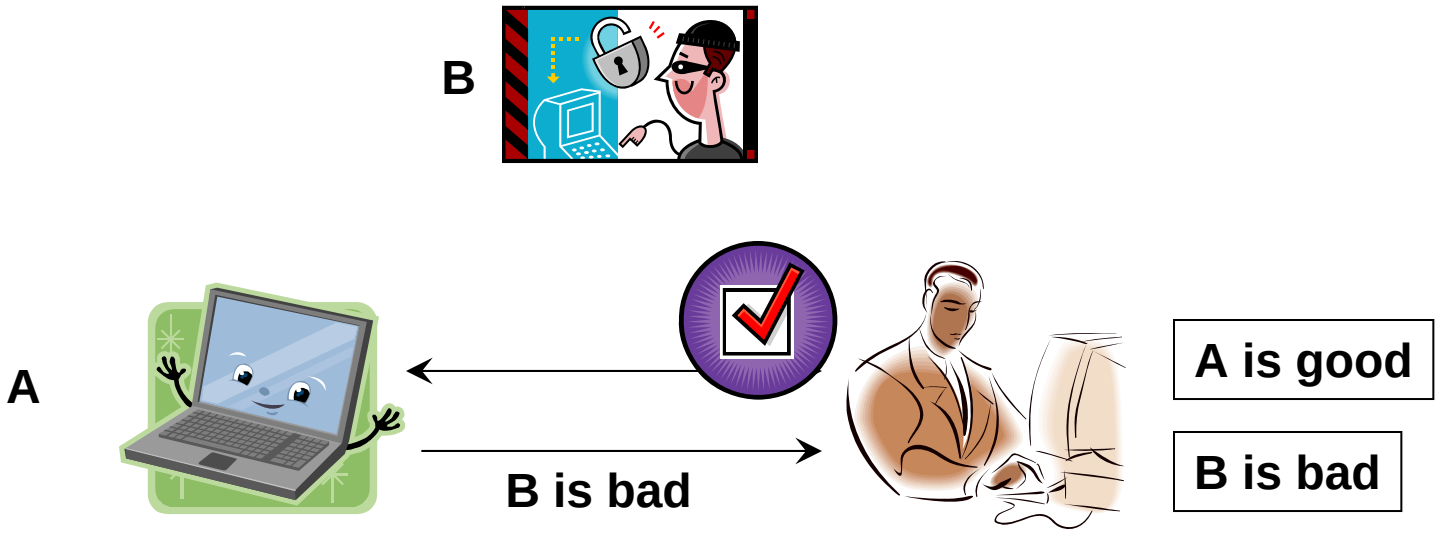
- Large-scale network applications are growing
  - Millions of users (EBay, Kazaa, Maze, Skype)
  - All involve peer-to-peer transactions / interactions
- The challenge
  - Users spread across many networks
  - Difficult to control and secure
  - Result: many users attacked and compromised by worms, mal-ware, Trojan horses
- To make it worse
  - Zero-cost identities: 1 attacker can control many users
  - Users are often selfish: free-riders

Are Reputations the Solution?



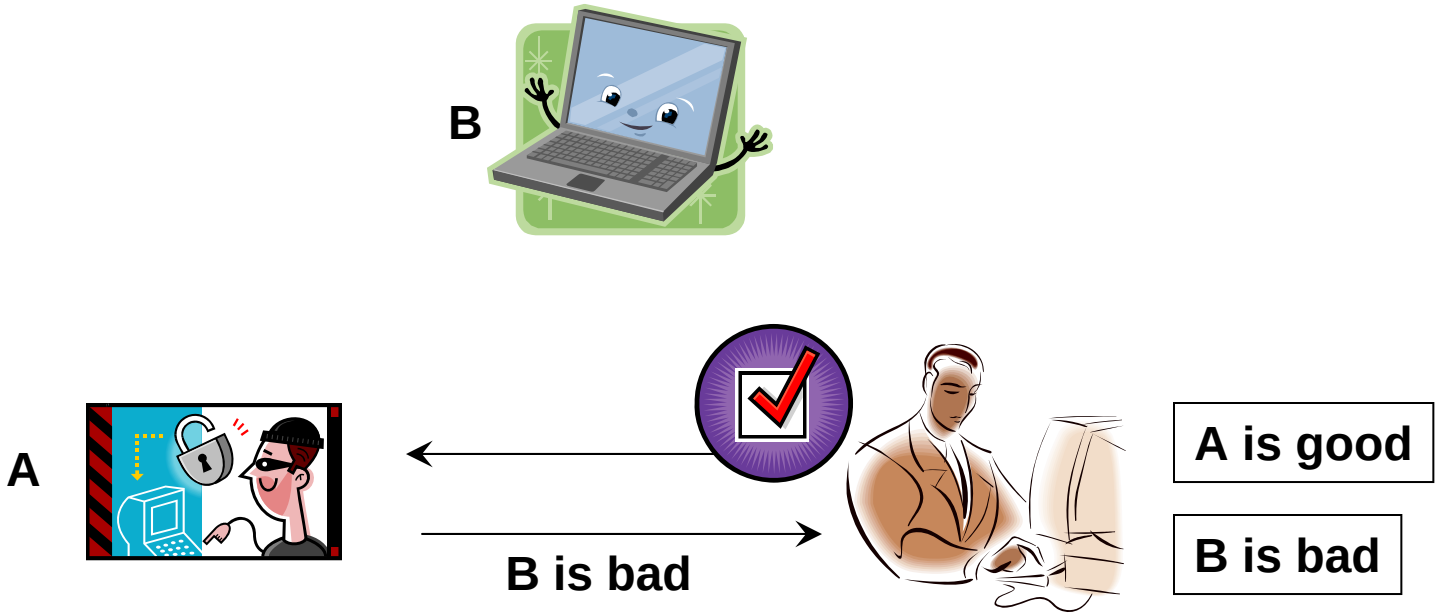
Correlated Trust

- Weighted model
  - Credibility as service provider ➔ Credibility as feedback provider



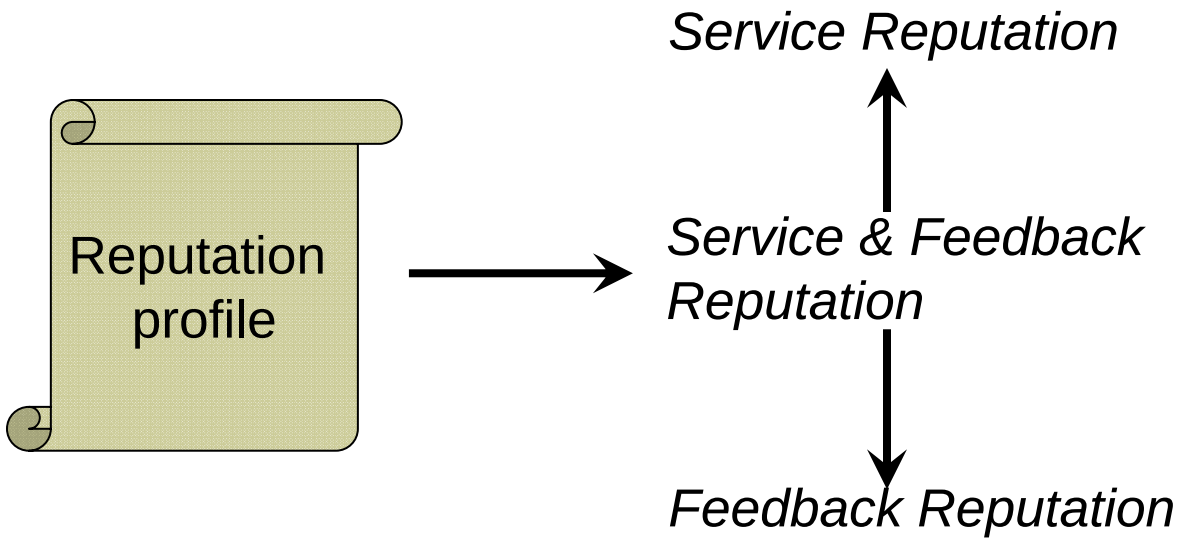
Correlated Trust, the Problem

- Malicious or “strategic” peers can manipulate correlated trust to badmouth others



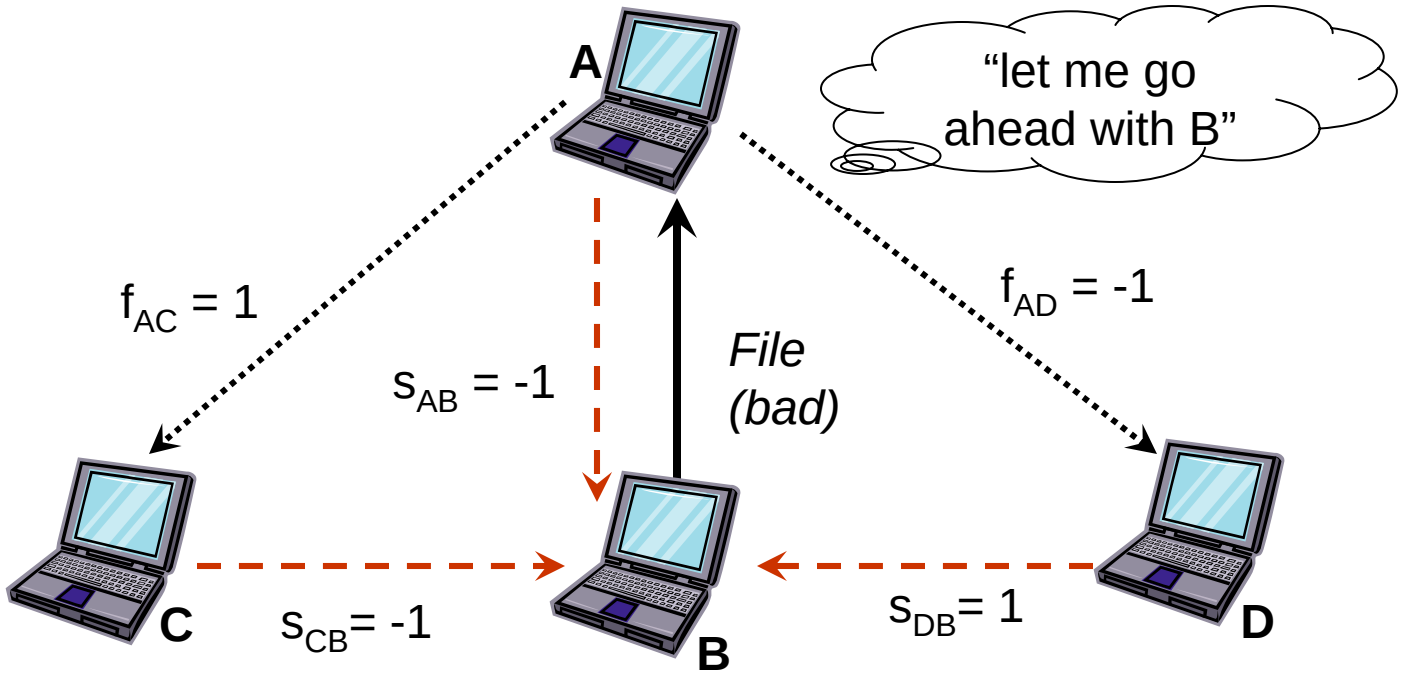
Our Proposal

- A novel, decoupled approach to account for a peer's credibility as service AND feedback provider
- Robust to unfair ratings



The Trust Model

- Each peer has two reputation ratings
  - A ***service rating*** (s-rating) and ***feedback rating*** (f-rating).
  - [-1,1] rating scale, 1 = good, -1 = bad



The Trust Model (contd.)

- Decouple service and feedback trust
  - Avoid strategic manipulation
- Weigh recent feedback more heavily
  - Account for dynamic peer personalities
  - α and β used to control time decay

$$s\text{-}rating(u) = \alpha * s\text{-}rating(u) + \beta * (r_u * f\text{-}rating(i))$$

$$f\text{-}rating(u) = \frac{1}{n_u} * \sum_{i=1}^{n_u} f_u * f\text{-}rating(i)$$

Evaluation via Simulations

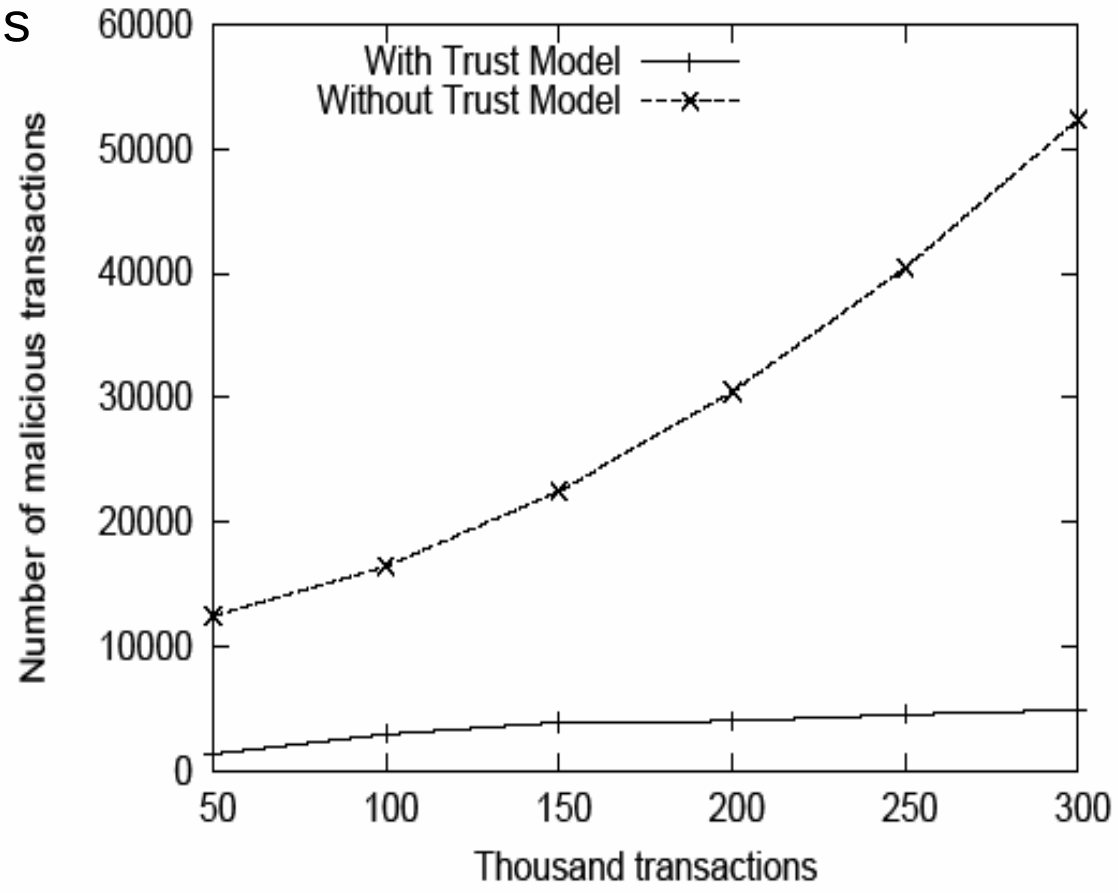
- Evaluation metrics
  - Effectiveness of reputation systems
  - Effectiveness of decoupled vs. correlated trust
- C simulator built on Stanford Graph Base
  - GT-ITM topologies
  - Peer community
    - Honest (good service, honest feedback)
    - Dishonest (bad service, dishonest feedback)
    - Strategic (good service, bad feedback)

Simulation Parameters

Parameter	Value Range	Default
Size of Network	50-1000	500
% of honest peers	0-100	60
% of malicious peers	0-100	40
% of strategic peers	0-100	0
# of queries per experiment	50-1000	500
Number of values per data point	5	5

Effectiveness against malicious behavior

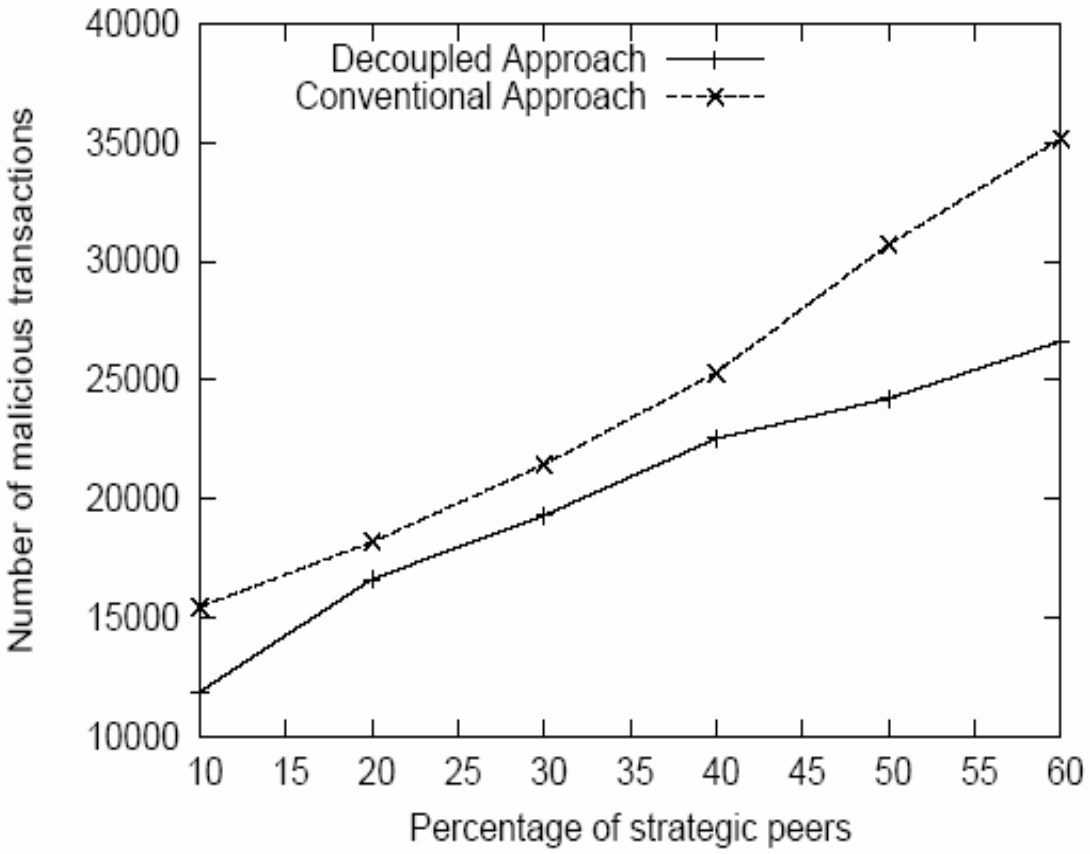
- Measuring malicious transactions
  - w/ our model
  - w/o our model
- 40% dishonest nodes



Benefits of decoupling trust

- Malicious transactions in networks with a conventional trust model and our decoupled model

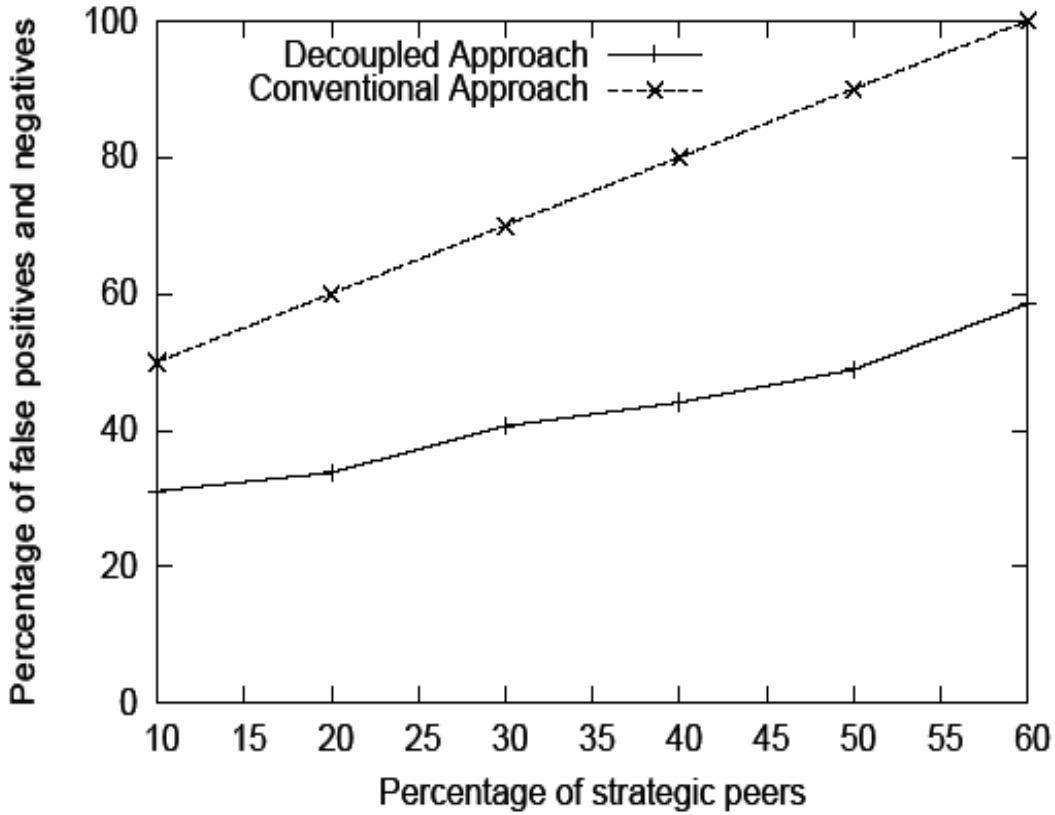
- 40% dishonest
- Vary % of strategic nodes



Benefits of decoupling trust

- False positives and negatives in a network with a conventional trust model and our decoupled model

- 40% dishonest
- Vary percentage of strategic nodes



Related Work

- PeerTrust
  - *Personalized similarity* measure
  - Statistically hard to find common past partners
- CONFIDANT
  - A node's referral is interpreted subjectively per node
  - Nodes only measure reputation of local neighbors
  - Specific to mobile ad hoc routing

Conclusions and Ongoing Work

- Proposed solution is robust to
  - Unfair ratings
  - Dynamic peer personalities
- Open problems
  - Group collusion
  - Sybil Attacks
- Recent work
  - Confirmed impact of our work on Maze dataset
    Significantly improves reputation accuracy

Questions, comments?

For more about UCSB and our work

http://www.cs.ucsb.edu/~ravenben

Or e-mail: ***ravenben@cs.ucsb.edu***