Distributed Trust Management in Autonomic Networks

Tao Jiang and John S. Baras

Motivation

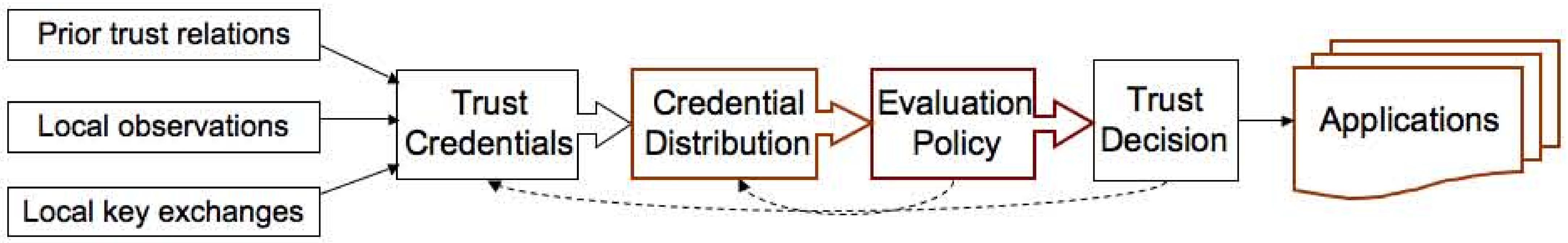
- Communication networks have been involved to be so complex that people, who created them, cannot control them.
- Future vision: to understand and control such complexity.
- Network science
  - The Internet and other communication networks
  - Social networks
  - Biological networks

⇨ **They are autonomic.**

Trust in Communication Networks

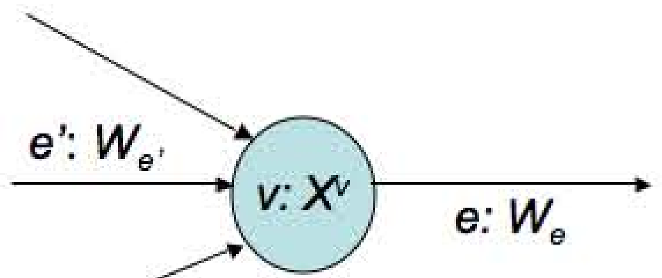
Traditional networks	Autonomic networks
Internet, cellular networks	MANETs, P2P
Centralized trusted authority	No trusted centralized authority Uncertainty and incompleteness Local information exchange Distributed computation

- Objective: use mathematical analysis to understand and predict the emergent behaviors of trust management systems in autonomic networks.
- Trust Management System in Autonomic Networks:



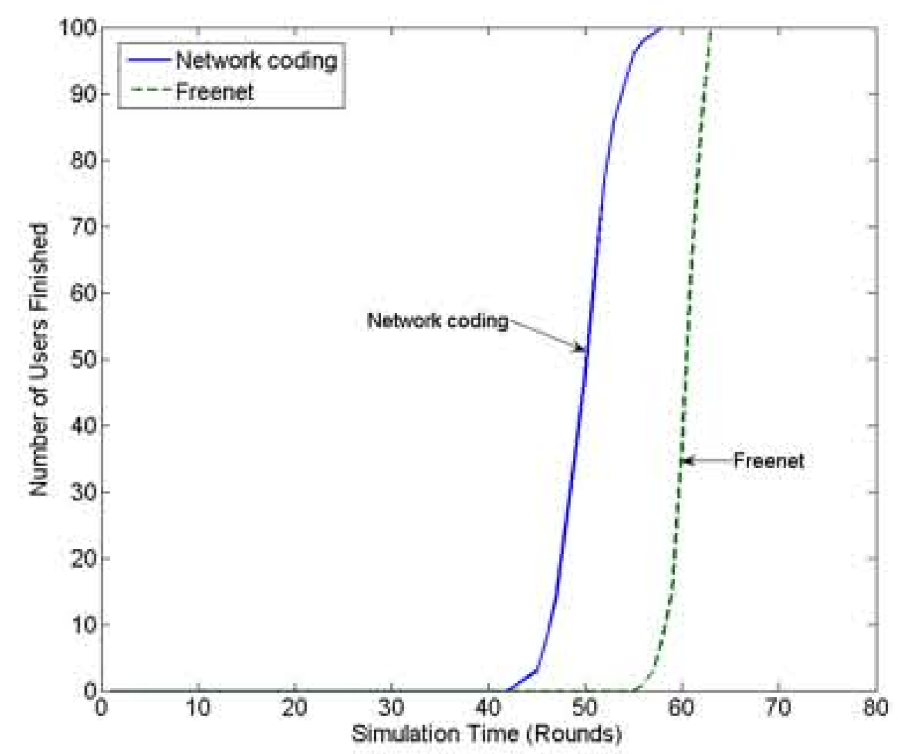
Trust Credential Distribution

- No centralized trusted party; trust credentials are scattered in the network.
- Problems:
  - Where and how to find all needed credentials?
  - Where and how to store credentials such that searching is efficient?



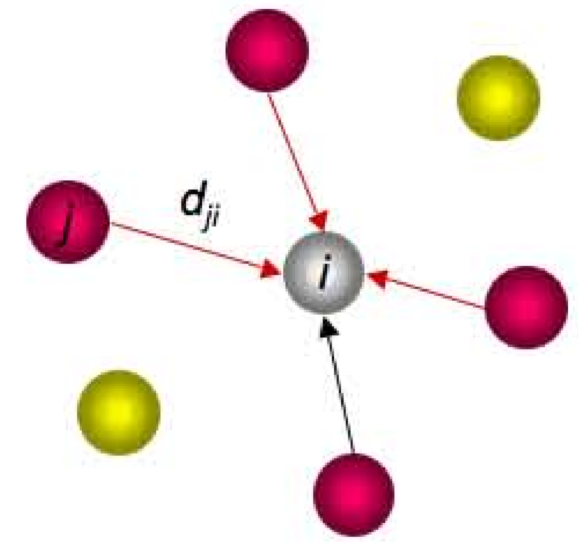
$$W_e = A_e \vec{X}^v + B_e \vec{W}^v = C_e \vec{X}$$

- P2P file sharing:
  - The problem of trust credential distribution shares many characteristics of P2P file sharing systems (Freenet).
  - Network coding based file sharing has been shown to be efficient and based on local information only.



- **Network Coding Based Scheme**
  - Extremely simple to implement
  - Only local information exchange
  - Easy for discovering new credentials
  - Small storage requirement
  - Efficient distribution

Trust Evaluation Policy



- The trustworthiness of an agent is based on other peers' opinion
  - The most straightforward scheme is to ask neighbors to "vote" for it.
  - Voters: neighbors with positive trust value are qualified as legitimate voters.
  - General voting rule: $s_i = f(d_{ji}, s_j, \forall j \in N_i, s_j > 0)$.
- **Stochastic voting:**

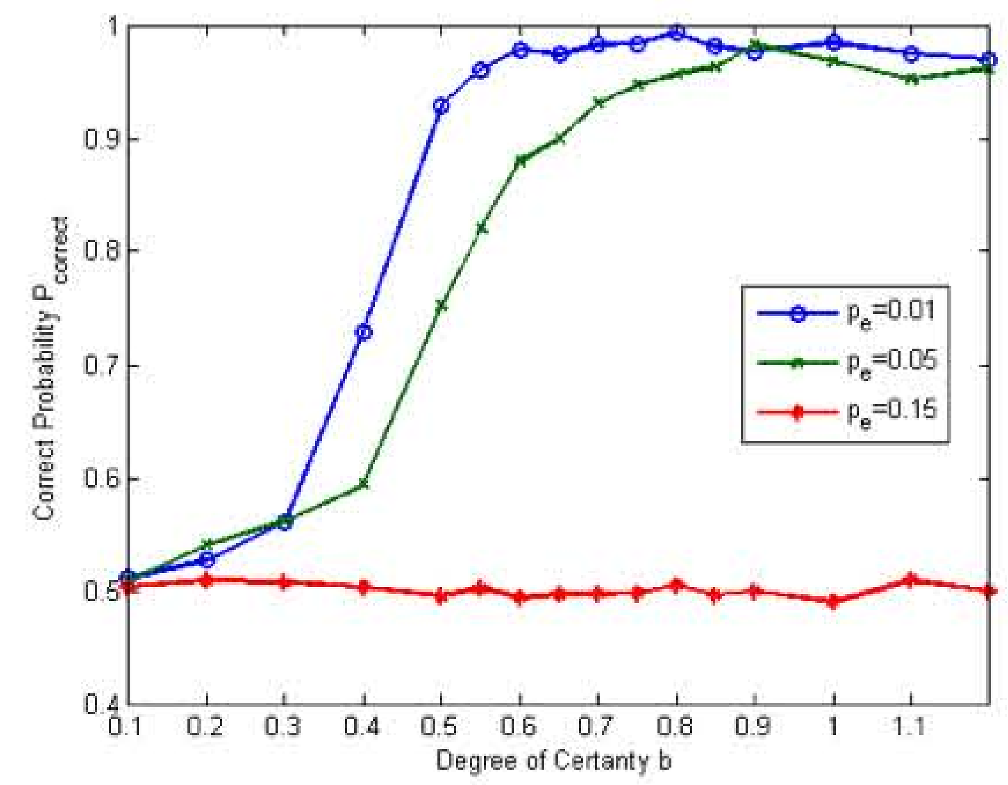
$$\Pr[s_i(k+1) \mid s_j(k), j \in \hat{N}_i] = \frac{\prod_{j \in N_i} \Pr[d_{ij}, d_{ji} \mid s_i(k+1), s_j(k)] \cdot \Pr[s_i(k+1)]}{Z_i(k)}$$

- **Convergence:**
  - The update rule iterates over time. We are interested in the steady state.
  - The stochastic voting can be interpreted as a Markov chain. Under trivial conditions, it can be shown that the update rule converges to a unique stationary distribution.
- Criterion: probability of correct estimation.

Phase transitions in two parameters:

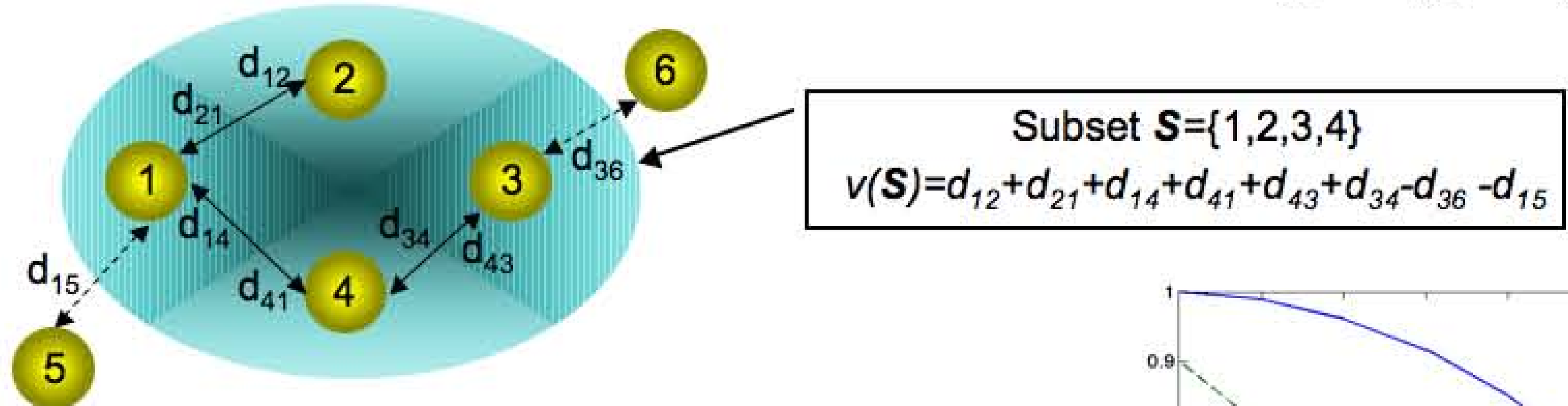
- Degree of certainty b
- Probability of error p_e

Theoretical analysis: results in the Ising model and the spin glass model, where $d_{ij} = J_{ij}$; replica method.



Trust and Cooperation

- The evaluation rule can be interpreted as dynamic (repeated) games:
  - d_{ij} can be interpreted as the worth of player j to player i.
  - The game is interpreted as a cooperative game, where nodes who collaborate with neighbors form a coalition.
  - The characteristic function of a coalition S is defined as $v(S) = \sum_{i \in S} \pi_i = \sum_{i,j \in S} d_{ij} - \sum_{i \in S, j \notin S} d_{ij}$.



Objective:

- to find what form or policy for d_{ij} can induce all (or most) nodes to cooperate: maximize the coalition.

Two solutions:

- Negotiation: Players with positive gain can negotiate with their neighbors by sacrificing certain gain.
- Trust: By introducing a trust mechanism, all nodes are induced to collaborate without any negotiation.