Trust in Distributed Networked Systems

Faculty: John S. Baras

Researchers: Vladimir Ivanov, Tao Jiang, ion Matei, Kiran Somasundaram, George Theodorakopoulos, Paul Yu, Shanshan Zheng

ISR @25 — The Institute for Systems Research, A. James Clark School of Engineering

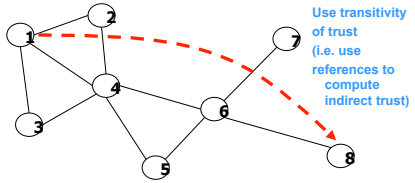
NETWORKS AND TRUST

- **Trust and reputation critical for collaboration**
- Characteristics of trust relations:
  - *Integrative* (Parsons1937) – main source of social order
  - *Reduction of complexity* – without it bureaucracy and transaction complexity increases (Luhmann 1988)
  - *Trust as a lubricant for cooperation* (Arrow 1974) – rational choice theory
- **Social Webs, Economic Webs**
  - MySpace, Facebook, Windows Live Spaces, Flickr, Classmates Online, Orkut, Yahoo! Groups, MSN Groups
  - e-commerce, e-XYZ, services and service composition
  - **Reputation** and **recommender** systems

INDIRECT NETWORK TRUST

User 8 asks for access to User 1's files.
User 1 and User 8 have no previous interaction

What should User 1 do?



Use transitivity of trust (i.e. use references to compute indirect trust)

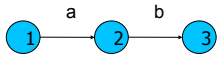
INDIRECT TRUST: SYSTEM MODEL

- System mapped to a **weighted, directed graph**
  - **Vertices** : entities/users
  - **Edges** : direct trust relations
  - **Weights** : $w(i,j)$ = How much i trusts j
- Establish an indirect trust relation, between users that have not had direct interactions
  - We assume that trust is **transitive (at least partially)**
- **Trust computation: path problem on a graph**
  - Information about j that is useful to $i \Leftrightarrow$ **Directed paths from i to j**
  - **Combine information along each path, and then aggregate across paths**

PARTIALLY ORDERED SEMIRING

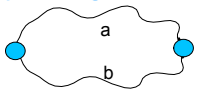
- Combined **along-a-path weight should not increase** :

$$a \otimes b \leq a, b$$



- Combined **across-paths weight should not decrease** :

$$a \oplus b \geq a, b$$



REPUTATION SYSTEMS

- **Reputation** is the opinion (more technically, a social evaluation) of the public toward a person, a group of people, or an organization
- **Online systems**: Slashdot, ePinion, Amazon, eBay, Yahoo!, Answers, Digg, Wikipedia, World of Warcraft, Bizrate, Elance.com, Alibris.com, MoneyControl.com
- **Naïve ideas**
  - By frequency of query words in a web page
  - By number of links from other relevant pages
- **Examples (Eigenvector- eigenvalue based)**:
- HITS algorithms, Hubs and Authorities algorithm (Kleinberg), PageRank (random walk model), SALSA,
- eBay Feedback, EigenTrust, BlogRanking -- EigenRumor

COMPUTING INDIRECT TRUST

- Path interpretation

$$t_{i\to j} = \bigoplus_{\text{path } p: i\to j} t^p_{i\to j}$$

- **Linear system interpretation**

$$t_{i\to j} = \bigoplus_{User\ k} t_{i\to k} \otimes w_{k\to j}$$

$$\vec{t}_n = W \otimes \vec{t}_{n-1} \oplus \vec{b}$$

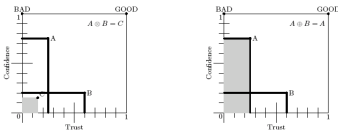
Indicator vector of pre-trusted nodes

- Treat as a **linear system**
  - We are looking for its **steady state**.

TRUST PATH SEMIRING

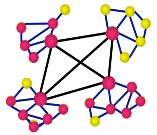
- 0 trust, confidence 1
- $\otimes$ is $(t_{ik}, c_{ik}) \otimes (t_{kj}, c_{kj}) = (t_{ik}t_{kj}, c_{ik}c_{kj})$
- $\oplus$ is

$$(t^{p1}_{ij}, c^{p1}_{ij}) \oplus (t^{p2}_{ij}, c^{p2}_{ij}) = \begin{cases} (t^{p1}_{ij}, c^{p1}_{ij}) & \text{if } c^{p1}_{ij} > c^{p2}_{ij} \\ (t^{p2}_{ij}, c^{p2}_{ij}) & \text{if } c^{p1}_{ij} < c^{p2}_{ij} \\ (\max\{t^{p1}_{ij}, t^{p2}_{ij}\}, c^{p1}_{ij}) & \text{if } c^{p1}_{ij} = c^{p2}_{ij} \end{cases}$$



TRUST DYNAMICS and LOCAL VOTING RULES

- **Trust and mistrust spreading**



Initial "islands" of trusts → Trust spreads → **Trust-connected network**

$$s_i(k+1) = f\left(J_{ji}, s_j(k) \mid j \in N_i\right)$$

- 'Generalized consensus' problems
- Spin glasses (from **statistical physics**), phase transitions

TRUST AWARE PROTOCOLS

- Trust aware NUM

$$-\max_x \sum_f U_f(x_f) \Longrightarrow \max_x \sum_f U_f(g_f x_f) \quad (\tilde{x}_f = g_f x_f)$$

- **Dual decomposition (log change all variables)**

$$L(\lambda,\nu,\tilde{x},x,\mu,g) = \sum_f \max_{x'_f}\left\{\nu_f x'_f - \lambda^f_{x'_f} e^{x'_f}\right\} + \sum_f \max_{\tilde{x}'_f}\left\{U'_f(\tilde{x}'_f) - \nu_f \tilde{x}'_f\right\}$$

Flow rates

$$+\max_{g'} \sum_f \nu_f g'_f$$

Routes

Schedule (MAC)

$$+\max_{\mu\in\Gamma} \sum_{(i,j)\in\mathcal{L}} \sum_{f\in\mathcal{F}} \mu^f_{ij}(\lambda^f_i - \lambda^f_j).$$

– **Dual objective function** $h(\lambda,\nu) = \sup_{\substack{x\in\Lambda \\ x_f = g_f \cdot x_f}} L(\lambda,\nu,\tilde{x},x,\mu,g)$

TRUST AWARE PROTOCOLS – MULTI-CRITERIA OPTIMIZATION

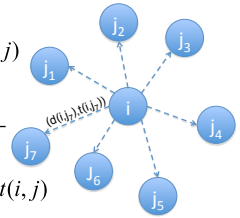
Bi-metric Network

- **Delay** of a path "p"

$$d(p) = \sum_{(i,j)\in p} d(i,j)$$

- **Trust** of a path "p" – bottleneck trust

$$t(p) = \min_{(i,j)\in p} t(i,j)$$



TRUST AWARE PROTOCOLS-MCOP

- How to build routing tables based on these metrics?
- The two metrics are not trivially comparable.

$$MCOP: \quad (\boldsymbol{P}_{SD}, f, X) / \theta / (\boldsymbol{R}^Q, \preceq)$$

Notation	Definition	Name
$x \leq y$	$x_i \leq y_i \quad i = 1,2,..,Q$	Weak component-wise order
$x < y$	$x_i \leq y_i \quad i = 1,2,..,Q$ and $x \neq y$	Component-wise order
$x \ll y$	$x_i < y_i \quad i = 1,2,..,Q$	Strict component-wise order
$x \leq_{lex} y$	$x_k < y_k \quad or \quad x = y \quad k = \min\{i : x_i \neq y_i\}$	Lexicographic component-wise order
$x \leq_{MO} y$	$\max_i x_i \leq \max_i y_i$	Max order

Pareto Optimal Paths – Edge Exclusion Algorithm

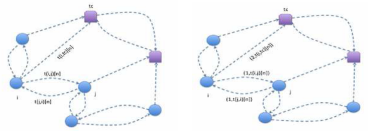
- Edge exclusion – From $G(V,E)$, remove all the edges whose $t(i,j) > \varepsilon$ to obtain a graph $G'(\varepsilon)$
- $G'(\varepsilon)$ contains paths which have all $t(i,j) \leq \varepsilon$
- We can also show that G' has all paths in G which have $t(i,j) \leq \varepsilon$ and only those

DISTRIBUTED KALMAN FILTERING and TRUST

Realistic sensor networks: Normal nodes, faulty or corrupted nodes, malicious nodes

- **Hierarchical scheme** – provide global trust on a particular context without requiring direct trust on the same context between all agents
- **Trusted Core**
  - **Trust Particles**, higher security, additional sensing capabilities, broader observation of the system,
  - Every sensor can communicate with one or more trust particles at a cost

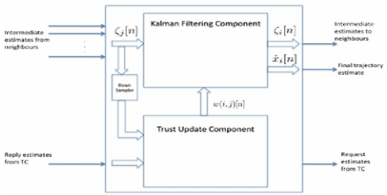
DISTRIBUTED KF and TRUST



Weighted Directed Dynamic Trust Graph $G_t(V, A_t)$ $V_{tc} \subset V$

Induced Graph $G(V, A)$ $w(i,j) = (c(i,j),\ t(i,j)[n])$

- Can use **any valid trust system**
- Can use **any Distributed Sequential Filter**
- Trust update mechanism: Linear credit and exponential penalty

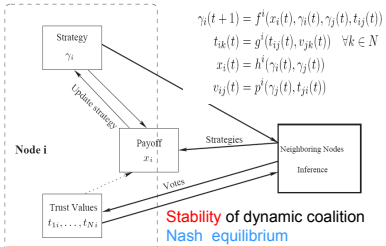


TRUST AND COLLABORATION

Two linked dynamics

- **Trust propagation and game evolution**

$$\gamma_i(t+1) = f^i(x_i(t), \gamma_i(t), \gamma_j(t), t_{ij}(t))$$
$$t_{ik}(t) = g^i(t_{ij}(t), v_{jk}(t)) \quad \forall k \in N$$
$$x_i(t) = h^i(\gamma_i(t), \gamma_j(t))$$
$$v_{ij}(t) = p^i(\gamma_j(t), t_{ji}(t))$$



Stability of dynamic coalition
Nash equilibrium

An example of constrained coalitional games

COMPOSITE TRUST

- Multiple Interacting Graphs
  - *Nodes*: agents, individuals, groups, organizations
  - Directed graphs
  - *Links*: ties, relationships
  - Weights on links : value (strength, significance) of tie
  - Weights on nodes : importance of node (agent)
- **Value directed graphs with weighted nodes**
- **Real-life problems: Dynamic, time varying graphs, relations, weights**
- **Ubiquitous example: Social networks over the web or over a communication network**