Modelling Interactions in Ubiquitous Environments

Mohamed Ahmed and Stephen Hailes

5th of May 2004
Environmental characteristics:

- Underlying systems are highly dynamic and mobile
- There is massive heterogeneity in the components and services available
- Components have a limited view of the global environment
- Principals have conflicting beliefs, desires and intentions
- There are no geographical boundaries and organisational boundaries are fuzzy

Determine the trustworthiness of individuals in such environments:

- What information can be used to determine this? And how can it be used?
- Where should this information be gathered from?
- What penalties can be in place to support acting on trusting intentions?
Traditional security

• Traditional trust management:
  – Centrally policed trust, through organisationally centralised authorities that determine the trustworthiness of individuals

• Assumes:
  – Widespread trust in these authorities
  – Availability
  – Enforceable penal system
  – Individuals cannot change their identities to avoid them

• Limitations:
  – Not fully supportable
Decentralised Trust Management

Situate decision making in the *local* context of interaction:

Based on information a *resource* can gather, the *risks* it faces, the potential *threat* posed by a *trustee* and the *local policies* of interaction

- **Identities**
  - Pseudonyms are cheap and may be ephemeral
- **Information Collection:**
  - Principals have different characteristics/policies
  - Heterogeneous incentives

Cooperating through trusting intentions is risky:

- Policies, Violations, Enforcement are local
Our Approach: Social Networks

If the consequences of interactions remain private; between a principal and a trustee

- Opportunism is a dominant strategy for malicious agents when interactions are infrequent or unpredictable.

• Solution
  - Transform the consequence of an interaction from private to public (without centralisation)
  - Leverage the embedded social network of principals
    - High value information
    - Credible threat of punishment

• Requirement
  - Create endogenous mechanisms that foster cooperation (between principals-witness and principals-trustees)
1. Assessing the intentions of trustees

2. Assessing the intentions of witnesses

3. Self organisation

How?
Assessing the intentions of trustees

• A signaling Game:

Given two agents; a Trustee \((T)\) and a Principal \((P)\). \(T\) has some private information \((t)\). On the basis of this information, \(T\) sends a message \((req)\) to \(P\). Based on the message \((req)\), \(P\) takes some action \((ac)\).
Our Translation

- **Utility of the principal:** \( U_p(t_x, req_x, ac_i) \)

- **Utility of the trustee:** \( U_x(t_x, req_x, ac_i) \)

- A principal's belief in the type of trustee:

\[
\mu(t_x \mid req_x) \equiv tr(a_p, a_x, \gamma_i, time)
\]
What is $t$?

- For each request $(req_x)$, the Receivers action $a^*(req_x)$ must maximise its expected utility, given the belief about which type of agent could have sent the request. Therefore $a^*(req_x)$ solves:

$$\max_{ac_i \in AC} \left( \sum_{t_x \in T} g \left( \mu (t_x \mid req_x), U_p (t_x, req_x, ac_i) \right) \right)$$
Which req?

For each type of agent ($t_x$), the Senders request $req^*(t_x)$ must maximise its expected utility, given the receivers (optimal) strategy ($a^*(req_x)$). Therefore $req^*(t_x)$ solves:

$$\max_{\forall req} \left( \left\{ U_x \left( t_x, req_x, a^*(req_x) \right) \right\}_{t_x \in T} \right)$$
Concluding remarks

We can create and use signalling mechanism to analyse the potential *type* of prospective trustees based on their *credentials*, the *requests* they make and their *history*.

Thank you for your attention,

All questions welcome
Our Translation

- A principal and a trustee: \( a_p \) and \( a_x \)
- Types of Agents: \( T = \{\text{Malicious, Good}\} \)
- Set of Resources a principal manages: \( \Gamma_p = \{\gamma_1, \gamma_2...\gamma_n\} \)
- Security categorisations of the resources: \( \text{sec}(OBJ, IMP) \)
- Set of Actions available on a resource: \( ACT_{\gamma_i}(act_1, act_2...act_n) \)
- A request for action upon a resource: \( \text{req}(a_x, act_i, \gamma_i) \)
- A set of actions available to a principal: \( \text{AC} = \{\text{grant, deny}\} \)
- Trust in a trustee: \( tr(a_p, a_x, \gamma_i, \text{time}) \)
Why do this?

• Large environments – potentially process a vast quantity of information

• Information from different sources
  – Partially redundant
  – Incomplete
  – Out of date
  – Contradictory

• Heterogeneous sources:
  – Different incentives
  – Credibility
  – Policies
What we need

- Methods of analysis that provide:
  - Reliable information evaluation
  - Support pre-emptive actions

- Distinguish between the types of information senders and the quality of the information sent.