

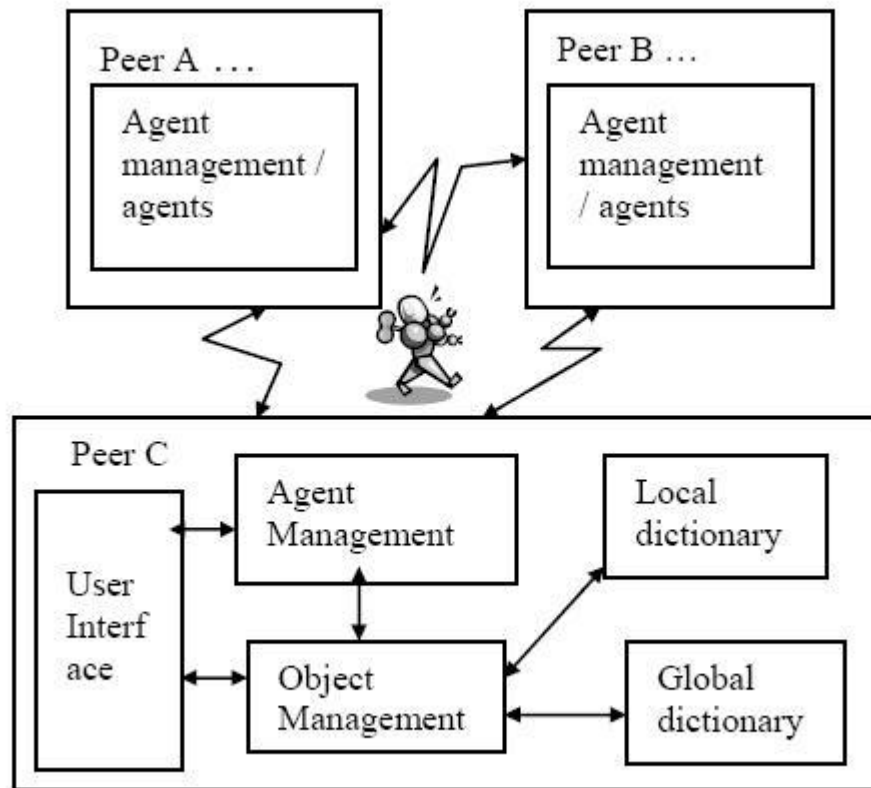
P2P – Security and Cooperation Strategies

Dorota Pawluczuk

Contents

- Security
 - BestPeer architecture
 - Parallel Dispatch Model
 - Serial Dispatch Model
 - Conclusions
- P2P from a different perspective

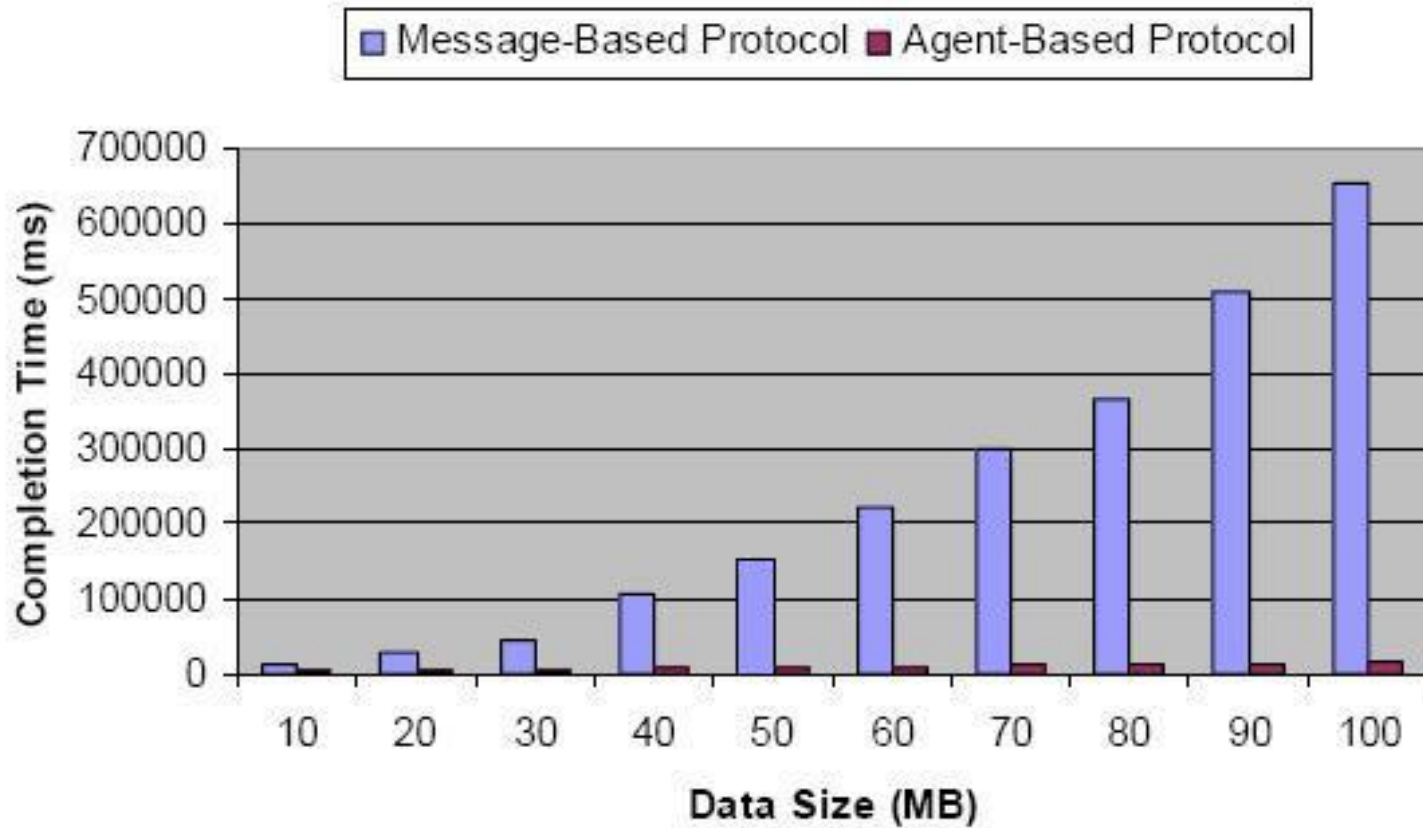
BestPeer – A P2P Based Data Management System



Efficiency of Mobile Agents in P2P Systems

- **message-based protocol** is a data-shipping strategy, remote data are transferred to the query node to be processed there
- **agent-based protocol** is a code-shipping strategy, the agent carries the processing code to the remote peer and performs remote execution. Only (partial) answers produced by the agent are then returned

Completion Time vs. Data Size



Challenges

- Secure connection between peers – the capability of each peer to identify the other participant in the connection
- Sensitive data managed or exchanged via applications must be protected
- The agents are prone to attack

Signcryption

- signcryption – operation, which has a significantly less computation cost than traditional “signature-then-encryption” technology
- Each peer own public and private key and corresponding certificates
- Each peer uses asymmetric keys to perform signcryption

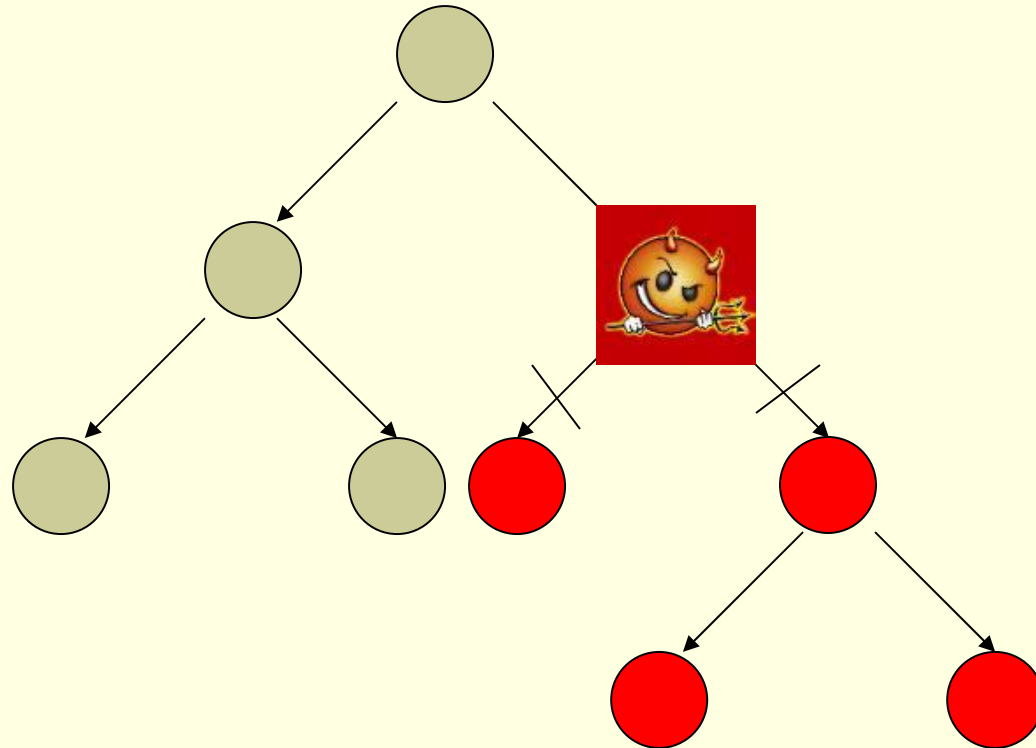
Parallel dispatch (binary model)

- Agents are dispatched in hierarchical way
- Each agent collects information from each peer and sends back the secured information to the initial peer
- Route is **predefined** and **signcrypted** by the public key of a target peer and a private key of Master Agent

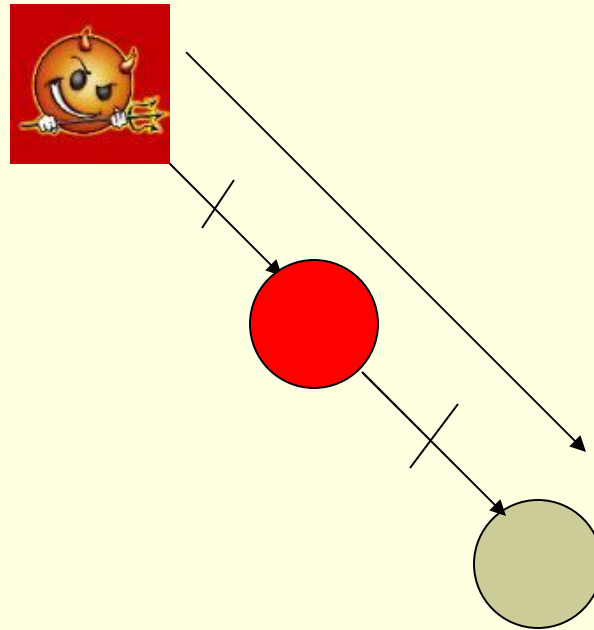
Types of agents

- Master Agent (MA) – starts the game
- Working Agent (WA) – local access to information; sends back answers to MA
- Primary Working Agent (PWA) – dispatches other mobile agents
- Peer's agent – dispatches PWAs
- SID – signcrypted, nested initiation data with description of tasks

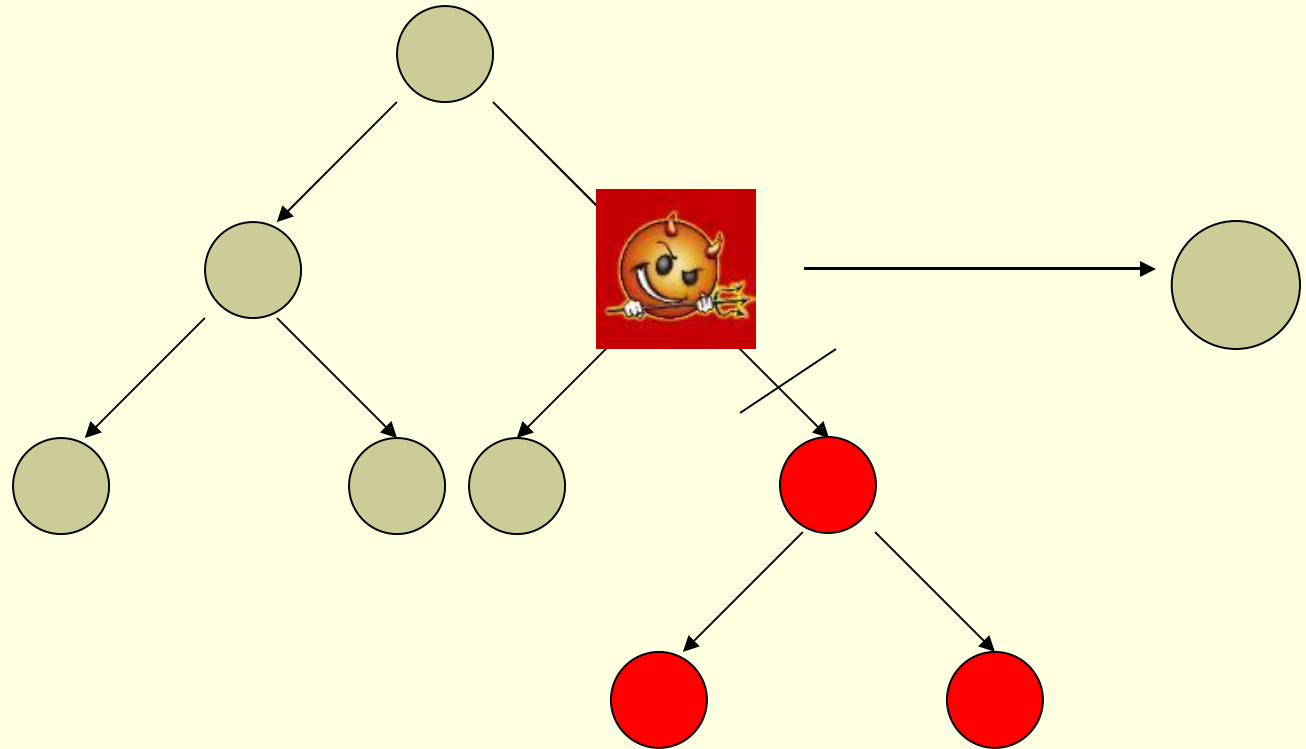
Preventing a PWA from dispatching a child agent



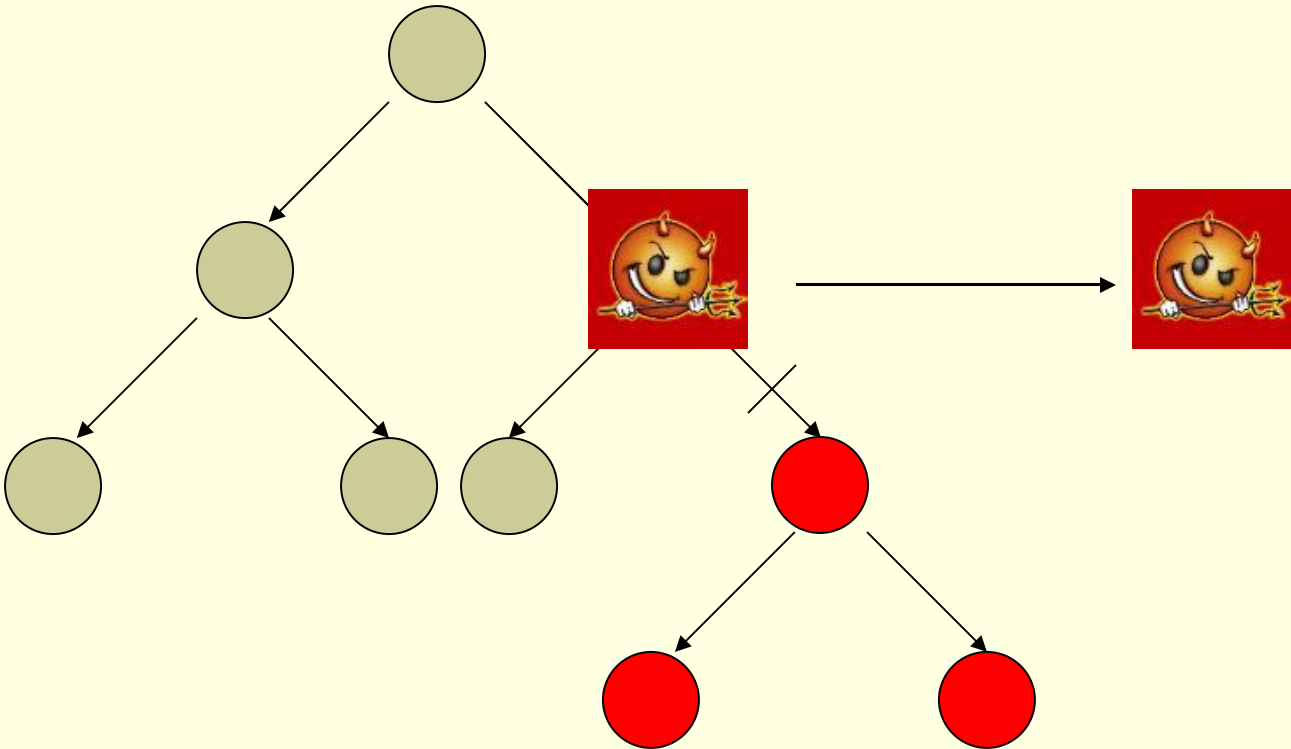
Route Skip Attack



Dispatching to the wrong peer



Collusion attack



Serial Dispatch Model

- Mobile agent carries the request signcrypted by the original peer
- Visits the other peers to collect information dynamically
- Each new peer modifies the message (i.e. adds the information) and performs signcrypting operation on the modified part to secure the provided information
- Route **not specified** beforehand

Security Issues in the Serial Dispatch Model (1)

- Protection of the Private Key of the Original Peer
 - agents do not carry the private key and any peer providing additional information only modifies the message part by performing the signcryption operation

Security Issues in the Serial Dispatch Model (2)

- Protection of Exclude Attack
 - assumption of non-conspiracy among peers
 - the public key of the next peer to be visited has been added in the generation of the signcrypted message
 - the order of peers agent visits will be fixed after agent returns back to the original peer

Security Issues in the Serial Dispatch Model (3)

- Prevention of the Disclosure of Collected Information
 - If any verifier, except the original peer and the peer that provides the information, wants to verify and unencrypt the information, it must get the private key of the original peer or of the peer that provides the information.
 - This is almost impossible based on the assumption of non-conspiracy among peers

Security - Conclusions

- The dispatch time complexity in the parallel dispatch model is $O(\log_2 n)$ whereas the complexity of the serial dispatch model is $O(n)$
- Parallel: no bottleneck, but visited peers must be predefined
- Serial: a mobile agent is more autonomous, but the original peer can evaluate the collected information only after the mobile agent returns back at the end of the overall process.

P2P

- Usually, P2P systems work on a uniform environment that does not allow for heterogeneity, inconsistency, and all the other phenomena one expects when dealing with distributed data
- Multi-Agent Systems (MASs) have addressed issues of coordination among autonomous, distributed agents for many years [Wooldridge and Jennings, 1995].
- MASs have been used to support the exchange of services between agents and/or platforms

Cooperative MAS with a flexible and dynamic task/agent assignment

- [Martín et al., 1999]
- Explicitly defines the role of a Peer Agent that uses P2P to solve tasks in a collaborative way.
- Each agent has a competence model of other agents
- Each agent is able to dynamically decide which agent to cooperate with.
- Each agent is able to execute tasks in several ways:
 - by itself
 - invoking a remote method inside another agent
 - transporting itself (i.e., the running code) to another place
 - and delegating a task to another agent.

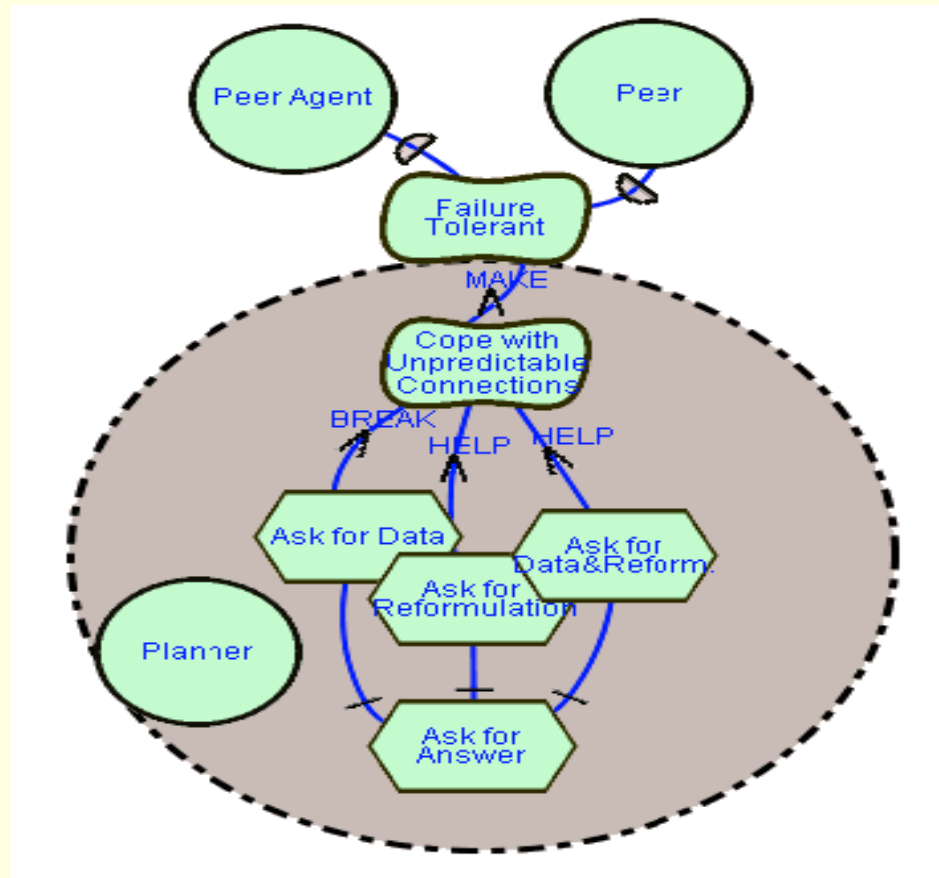
Strategic Dependency (SD) model


- Each peer agent plays one or more of the following roles to support the needs of its peer:
 - Wrapper (source interfacing)
 - Facilitator (searching and registration).
 - Mediator (reformulation and integration).
 - Planner (strategy generation).

The Strategic Rationale Model

- provides an intentional description of processes in terms of process elements and the rationale behind them
- forgoes that abstraction in order to allow a deeper understanding about strategic actors' reasoning about processes to be explicitly expressed
- describes the intentional relationships that are "internal" to actors, such as means-ends relationships that relate process elements, providing explicit representation of "why" and "how" and alternatives

SR Planner





Thank you for your attention