deepsia

Dynamic on-linE intErnet Purchasing System Based on Intelligent Agents

Multi-Agents System's
Security Developments

João Paulo Pimentão
Francisco Milagres
Pedro A.C. Sousa
Edson Moreira
Adolfo Steiger-Garção

Agenda

deepsia

- DEEPSIA's Overview
- Security aspects within DEEPSIA
  - Security needs identified and approaches
    - Agent Communication Language Security
    - Communication Security
- Future research

Project Objectives

deepsia

DEEPSIA (IST-1999-20483 project)
Dynamic on-linE IntErnet Purchasing System based on Intelligent Agents

Assist SME in the e-commerce process of finding the most suitable offer for their needs.

SME will find a user-friendly process for overcoming:

- **Individual purchases of items at “best” costs**
- **Finding new suppliers**

To drive "old data collection process" companies to address "new electronic data collection process" issues through the adaptation to an "e-access" of existing processes.

Business to Business (B2B) e-commerce models usually focus on SMEs as suppliers (virtual shops or marketplaces). DEEPSIA’a aim is the opposite.

Generic characteristics

deepsia

Purchaser- centred solution

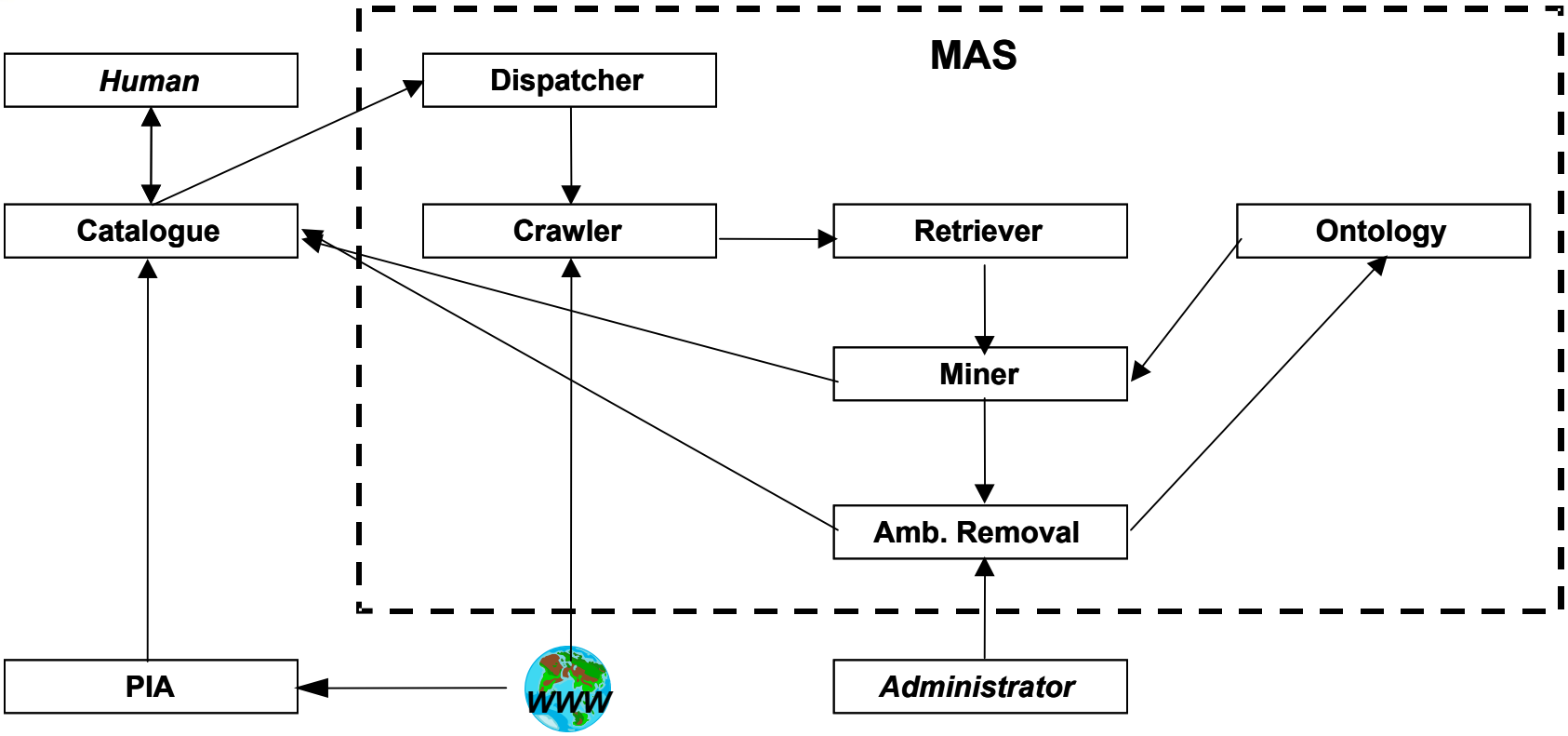
- Tailored to individual requirements
- User-friendly web interface based on a **purchaser-personalized catalogue**

The catalogue

- **Automatically updated** with information gathered from available e-business portals
- Set of **intelligent agents** which will look for data on the Web and process it

DEEPSIA's Architecture

deepsia



Security needs and approach

deepsia

Needs

Anonymity: the capacity to hide the final client from the queries he/she is performing;

Confidentiality: assure that the contents of the messages being exchanged remain hidden;

Reliability/Integrity: assure that the messages arrive intact as they left their origin;

Authentication of the sender: assure that the originator was who it was supposed to be;

Access Control: to the information beign exchanged;

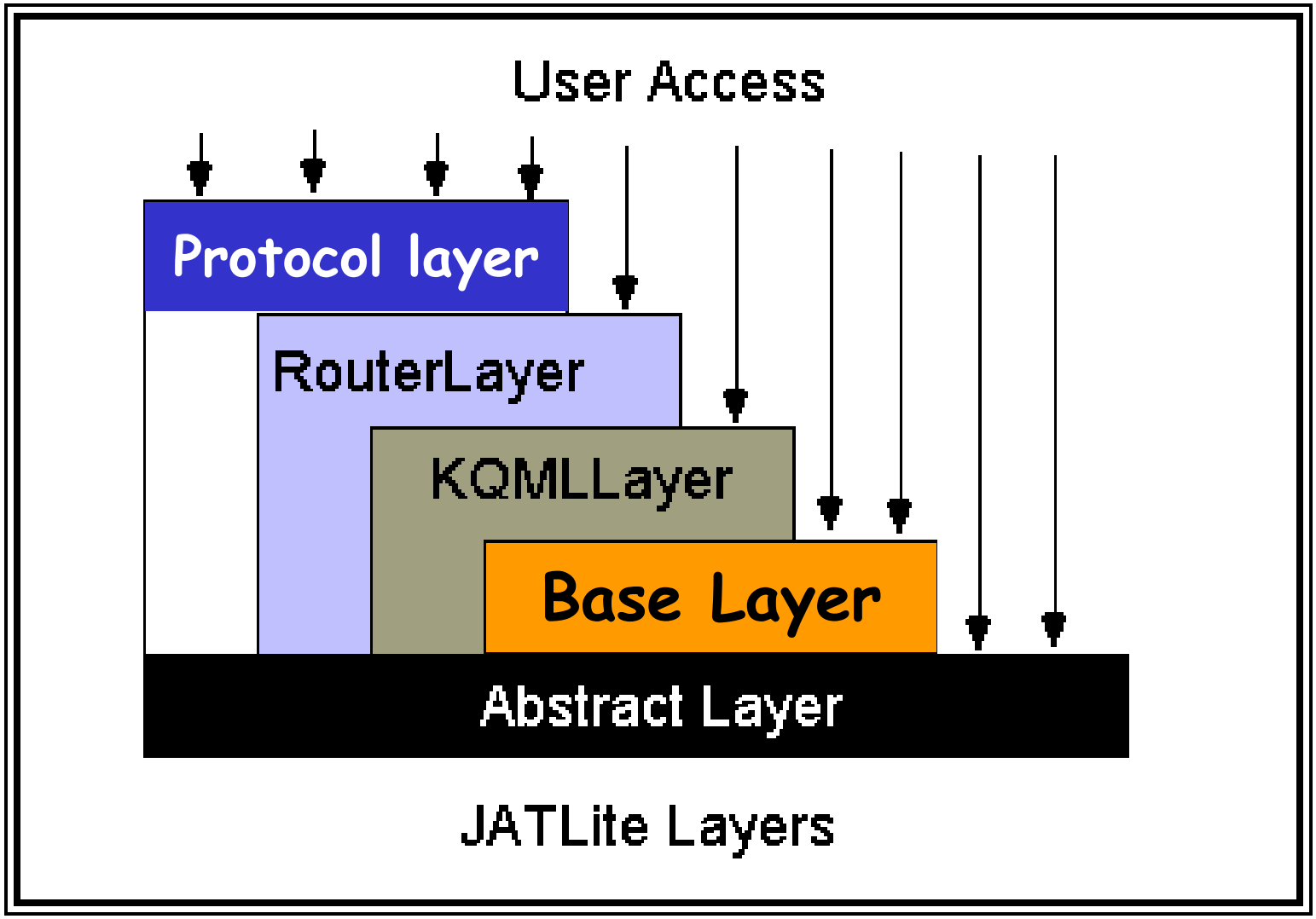
Availability: of the whole system.

Developments under way:

- *Agent Communication Lang. Security:* KQML – ACL Security, by USP
- *Message content Security:* "Split and Merge", by UNINOVA

JATLite Layers focused

deepsia



ACL Security - KQML

deepsia

- Based on Thirunavukkarasu, Finin and Mayfield *Secret Agents* proposal (UMBC, 1995)
- Some changes to KQML to improve its **authentication of message sender, message integrity and privacy of data**
- And security on **JATLite Base layer** for a transparent KQML communication

Communication Security: The Split and Merge way

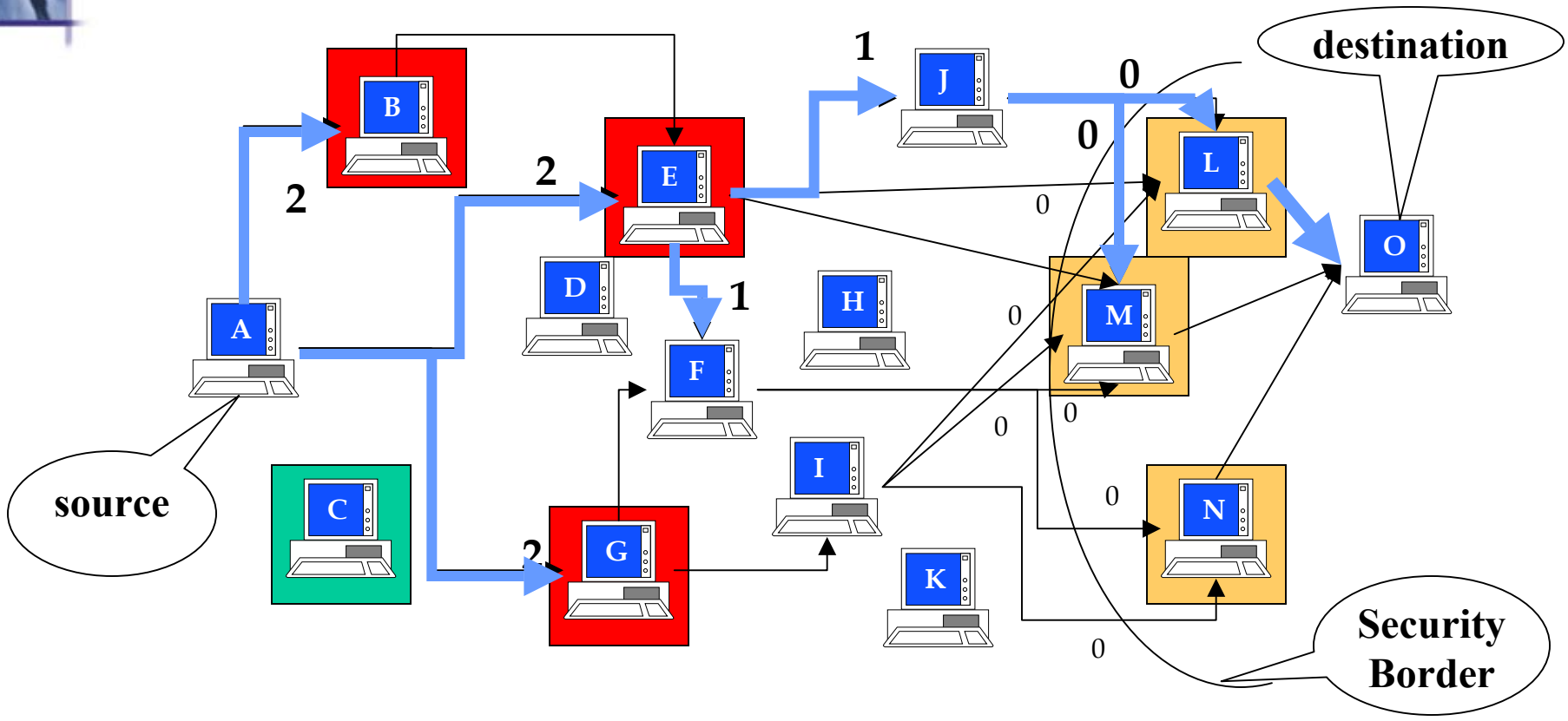
deepsia

In short:

- Split the message into fragments
- Send them through different paths
- Repeat the splitting at each node
- Reassemble the message at the destination

Split and Merge

deepsia



Future researches

deepsia

- After the final prototype:
  - Impact analysis of **ACL substitution** (FIPA ACL instead of the *ancient* KQML)
  - Definition of **specific security requirements** regarding to full system security and its interfaces within agents
  - Implementation of an **hybrid security model** with a default and secure ACL (FIPA) in partnership with other research groups (e.g., Agentcities)

Further information

deepsia

- http://www.deepsia.com
- Group contacts:
  - UNINOVA
    - *João Paulo Pimentão or Pedro A.C. Sousa*
      - pim@uninova.pt or pas@uninova.pt
  - University of São Paulo
    - *Francisco Milagres or Edson Moreira*
      - francisco@milagres.com or edson@icmc.usp.br