

# CERIAS

the center for education and research in information assurance and security

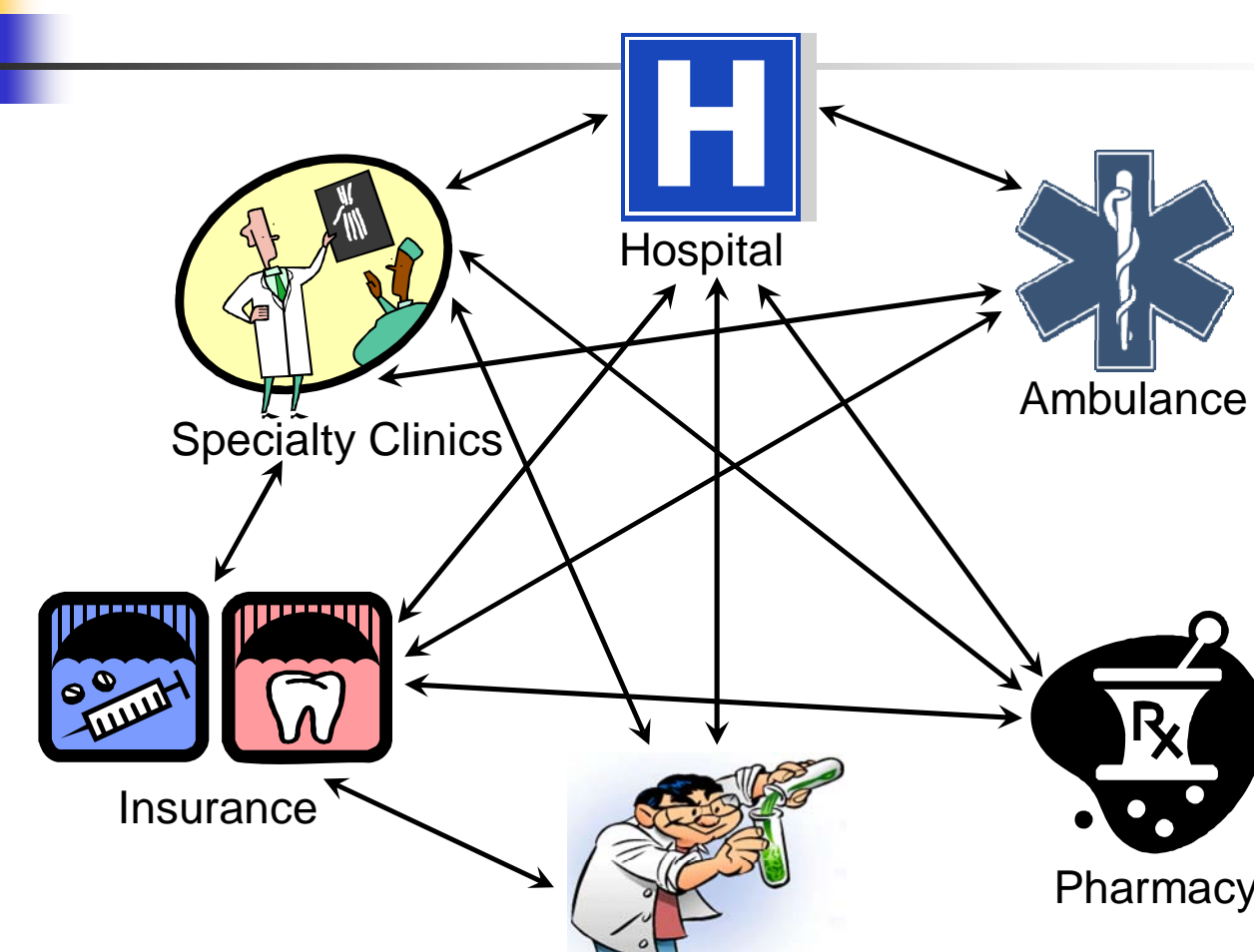
## Secure Collaboration in Mediator-Free Environments

Mohamed Shehab

Elisa Bertino

Arif Ghafoor

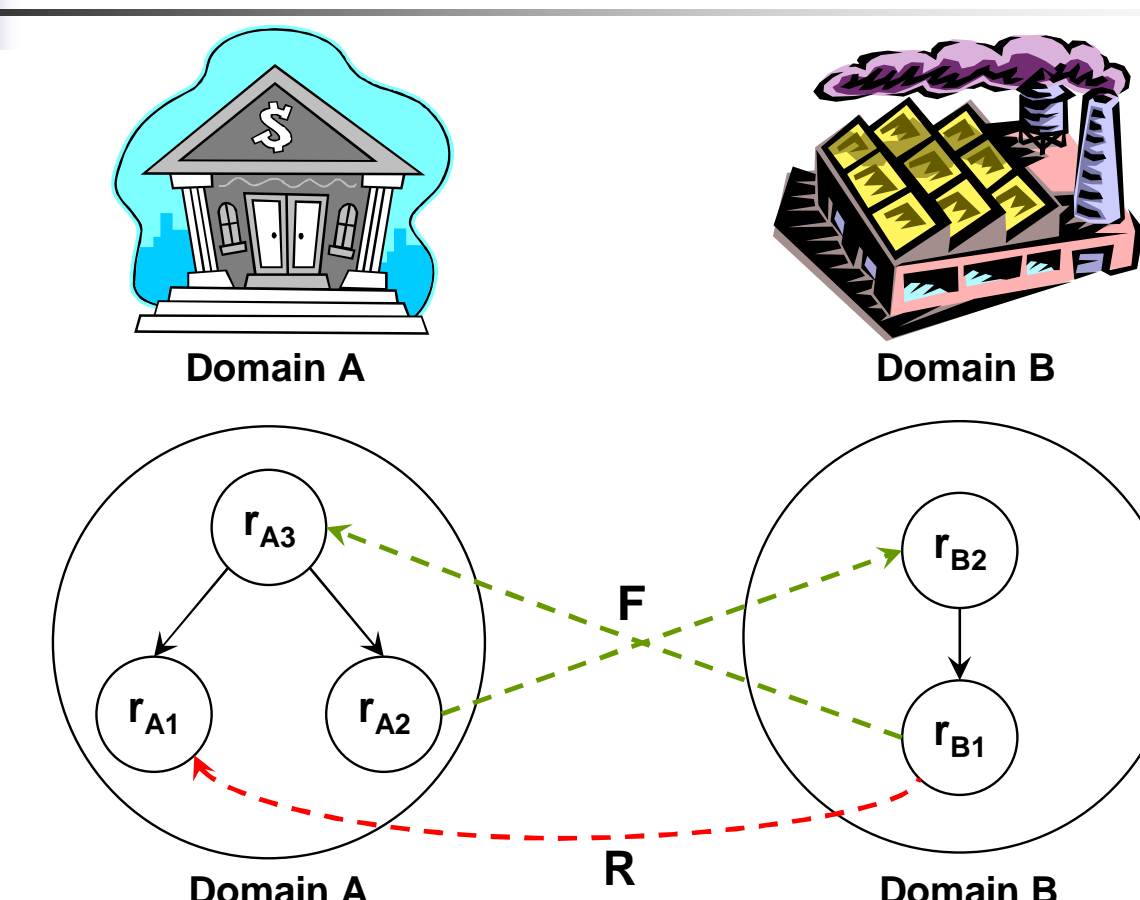
### Why Collaboration ?



### Secure Collaboration

- Given  $n$  domains,  $G_i = \langle V_i, A_i \rangle, i=1, \dots, n$ , the interoperability between these systems is achieved by introducing:
  - Cross links (F):** Set of pair wise mappings between roles in different domains (permitted access).
  - Restricted Links (R):** Set of prohibited mappings between roles in different domains.

### Secure Collaboration

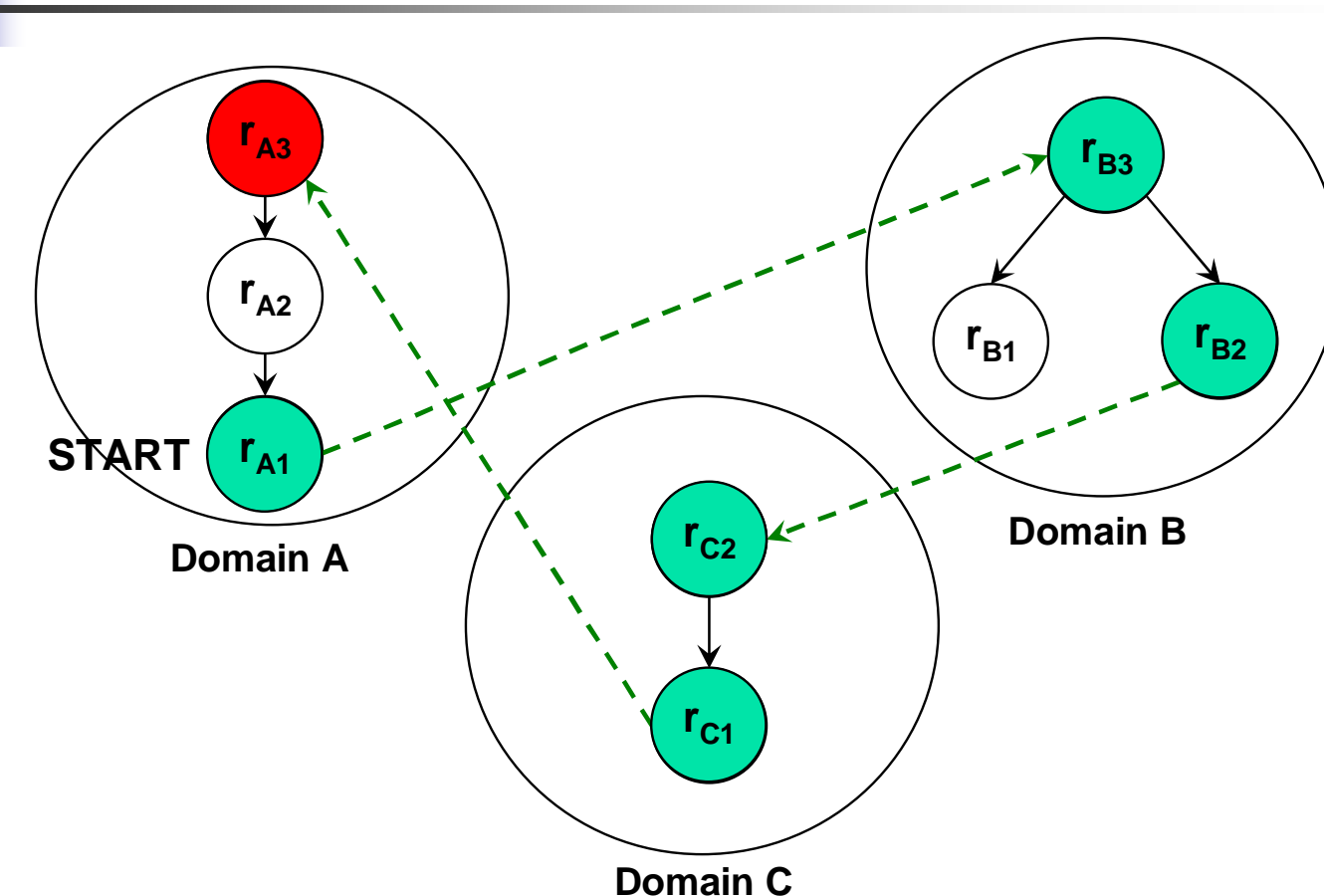


### Secure Collaboration

- Secure interoperability should satisfy:
  - Principle of Autonomy:** requires that any access permitted within an individual domain must also be permitted under secure interoperation.
  - Principle of Security:** requires that any access not permitted within an individual domain must also be denied under secure interoperation.

### Secure Collaboration Requirements

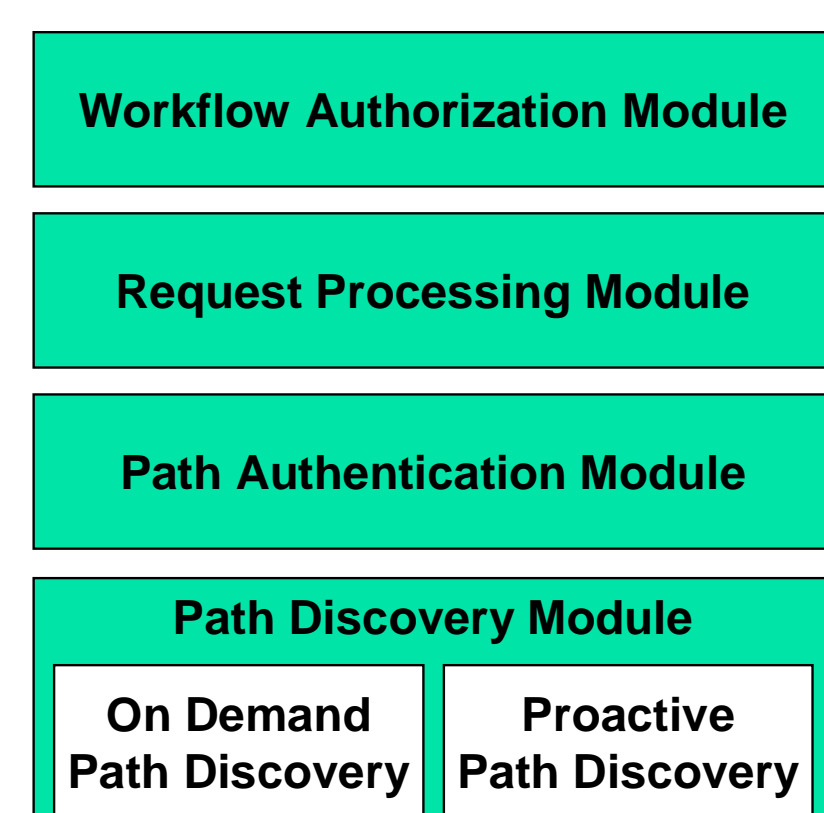
### Secure Path Requirements



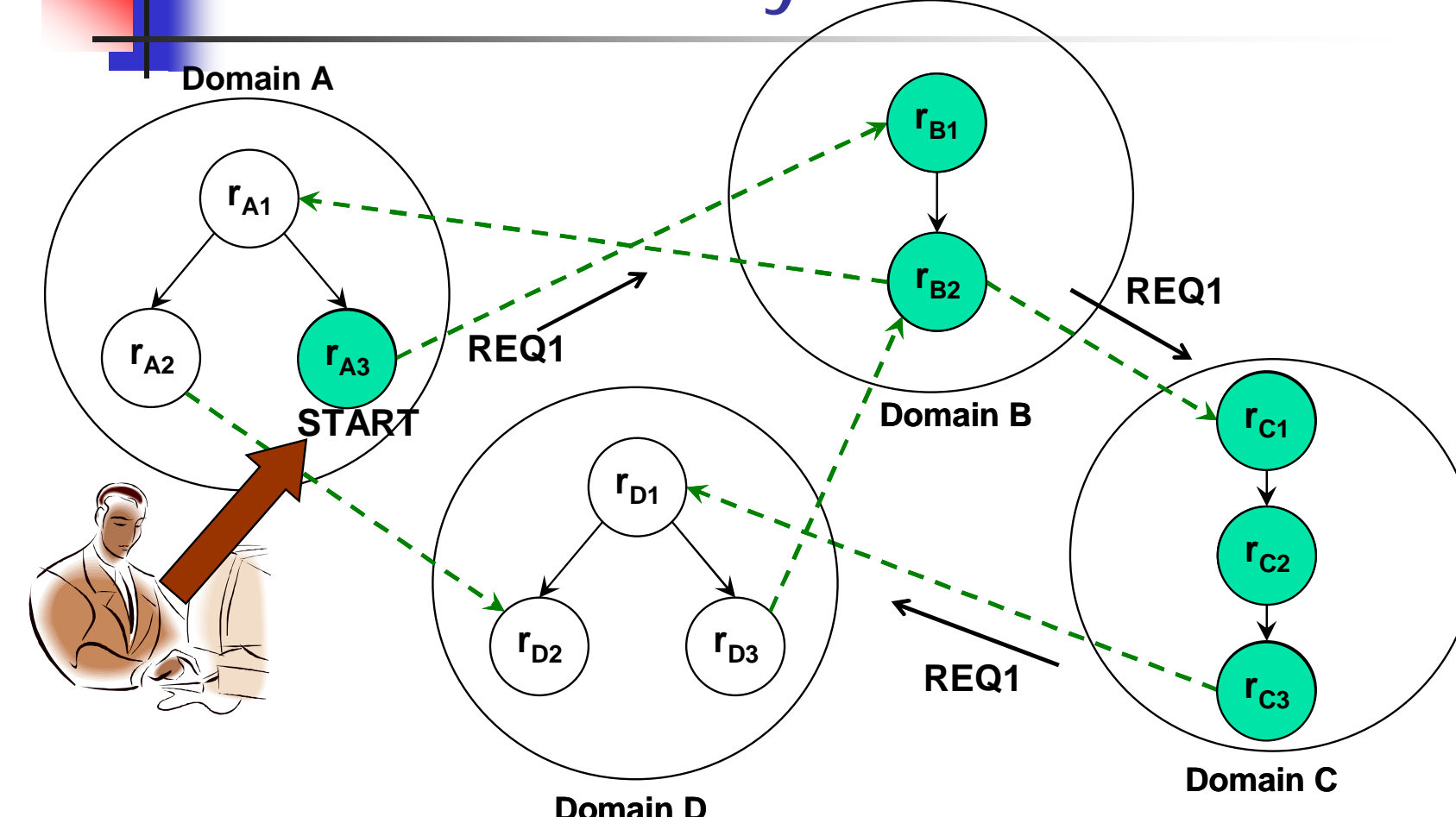
### Assumptions

- Each domain  $D_i$  is only required to know:
  - Its domain policy,  $G_i = \langle V_i, A_i \rangle$ .
  - The cross links with other domains,  $F_i \subseteq F$ .
  - The restricted links with other domains,  $R_i \subseteq R$ .
- The user's access path is attached with user requests.

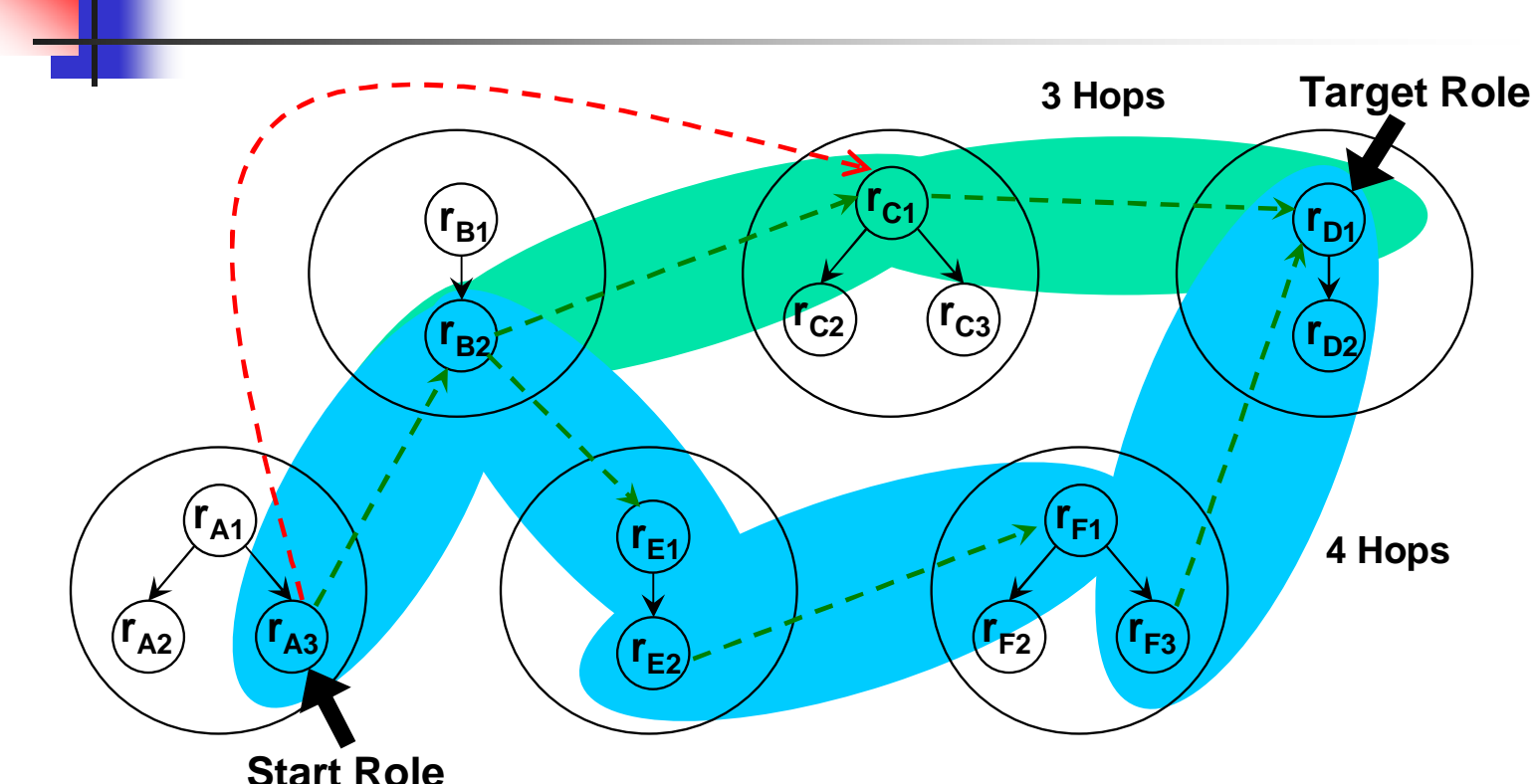
### Framework for Secure Mediator-Free Collaboration



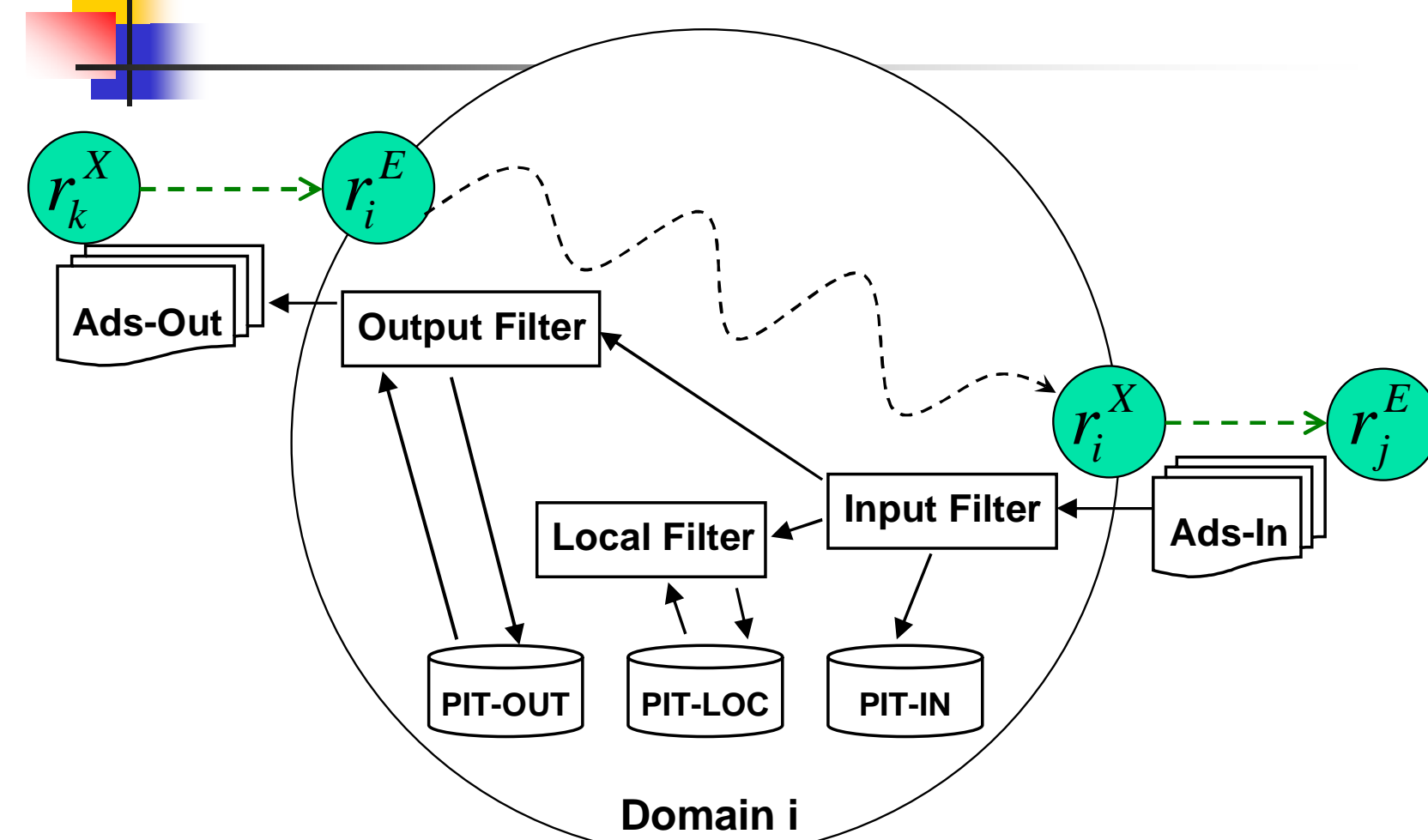
### Path Discovery: On-Demand



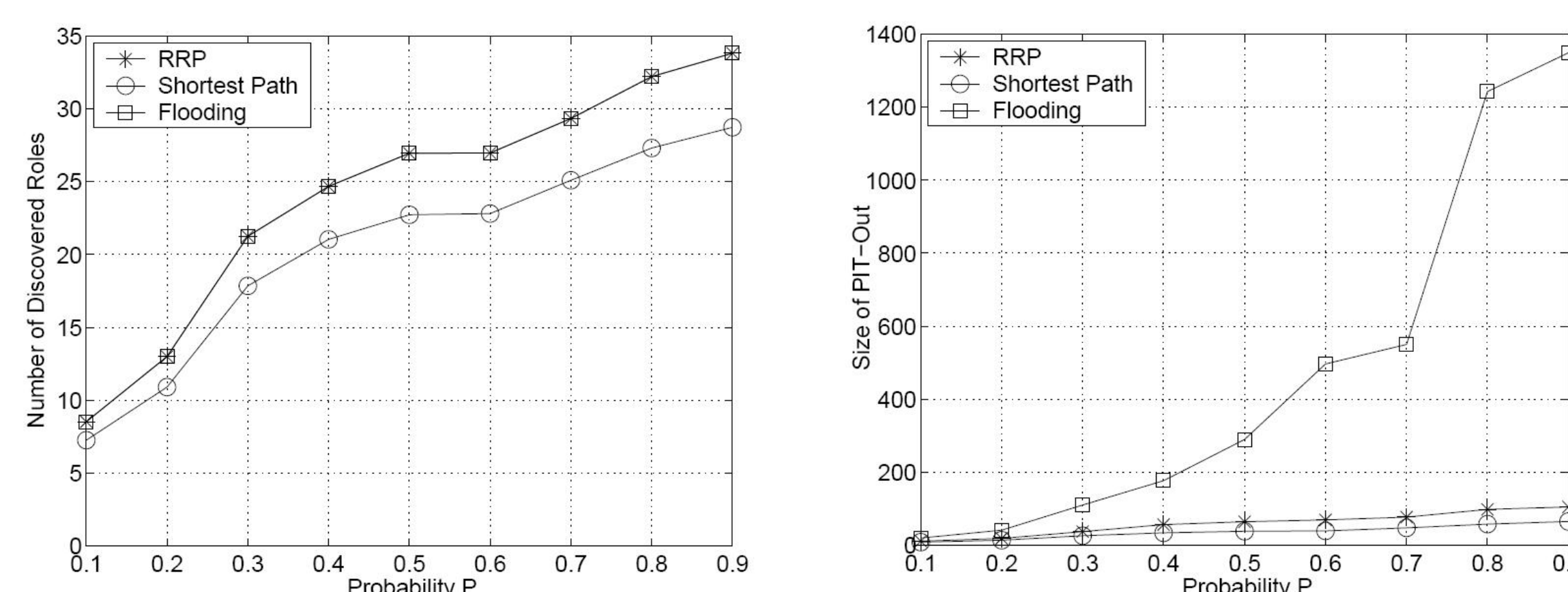
### Path Discovery: Proactive



### RRP Path Advertisements



### Experimental Results



### Private UDDI Registry

