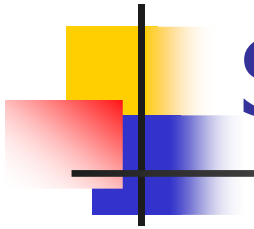
Athens University of Economics and Business, Greece,
Dept. Of Informatics
MMLAB

Providing Anonymity Services in SIP

PIMRC 2008

Sept. 15, Cannes, France

L. Kazatzopoulos, K. Delakouridis, G.F. Marias
lkazatzo@aueb.gr, kodelak@aueb.gr, marias@aueb.gr

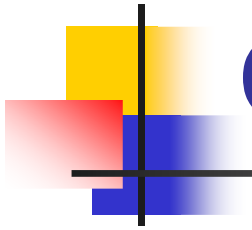


Session Initiation Protocol - SIP

- widely used for setting up and tearing down multimedia communication sessions (voice and video calls) over the Internet.
- Applications: video conferencing, streaming multimedia distribution, instant messaging, presence information
- creates, modifies, terminates two-party or multiparty sessions consisting of one or several media streams

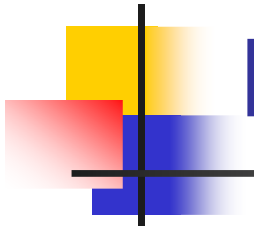
SIP – Levels of anonymity

- **caller's absolute anonymity**,
  - the caller identity cannot be exposed by any other entity, or the attacker
- **caller's eponymity only to the callee**,
  - the identity of the caller should be revealed only to the callee
- **caller's eponymity only to her/his provider**,
  - the identity of the caller should be revealed only to the his/her provider
- **caller's eponymity only to callee's provider,**
  - same as above, but for the peer's provider



Candidate PETs

- **Mixes**
  - **Pool Mixes**
  - **Stop and Go Mixes**
  - **Mixe-Nets**
- **DC-Networks**
- **Crowds**
- **Hordes**
- **Onion Routing**
- **Routing Through the Mist**



Evaluation criteria of PETs

- **Call establishment delay**
- **Cost**
  - **Computational**
  - **Communication overhead**
- **Scalability**
- **Protection level – robustness**
  - **Threats against anonymity**
- **Anonymity**
  - **of both caller and receiver**
- **Authentication**
  - **Supported or not?**

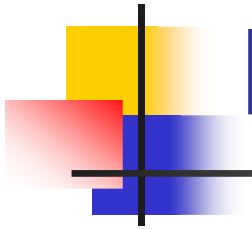
Evaluation criteria of PETs

	scalability	robustness	Call delay	Anonymity	Authentication	cost
MIXES	M	N	H	L	N	L
POOL MIXES	M	N	H	M	N	M
S & G MIXES	M	N	M	M	N	M
MIXNETS	M	L	M	H	N	M
DC-NETS	L	H	M	H	N	M
CROWDS	H	M	M	L	N	L
HORDES	H	M	M	L	N	M
O.R	H	H	H	H	N	H
R.T.T.M	H	H	M	H	Y	H

- **H: High**
- **M : Medium**
- **L : Low**
- **Y: Yes**
- **N: No**

Best candidate: Mist

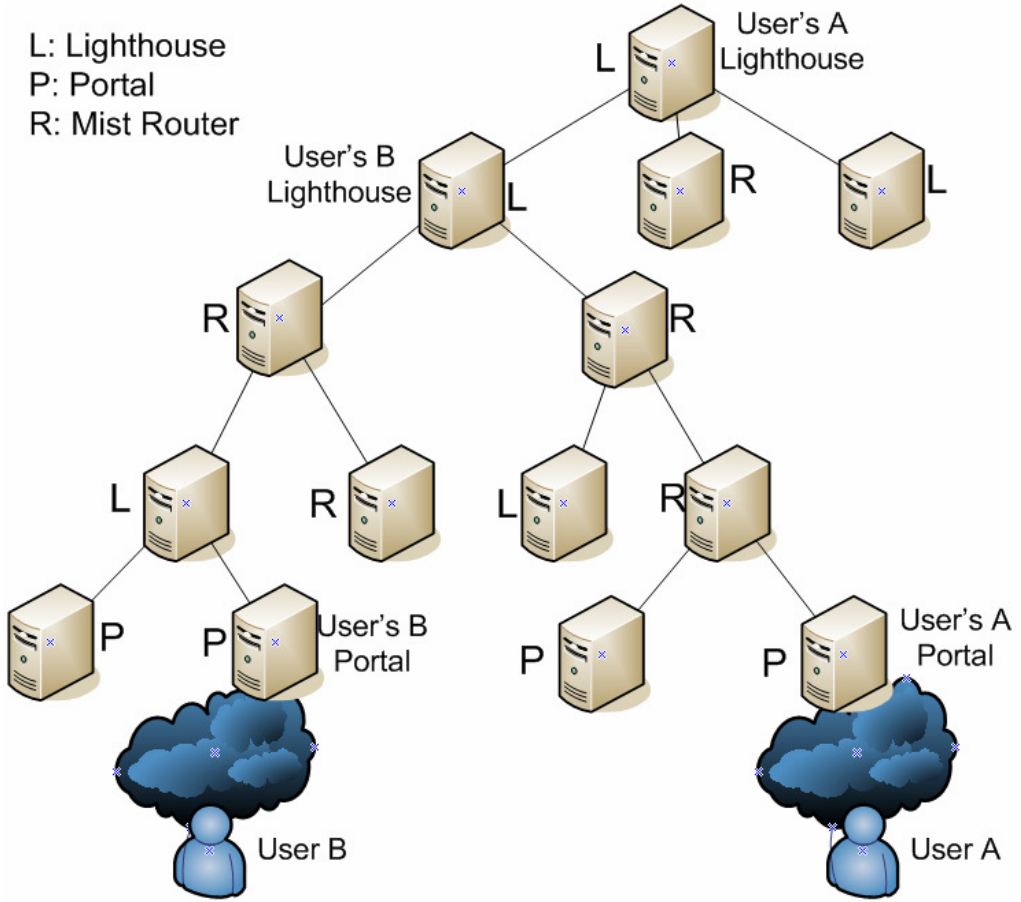
- Mist Routers is Hierarchical Structure
- Handle based communication
- Portal:
  - Mist Router – leaf node
  - Knowledge of user's positions but not user's ID
- Lighthouse:
  - Mist Router – Portal's ancestor
  - Semi-trusted intermediate
  - Knowledge of user's ID but not user's physical position



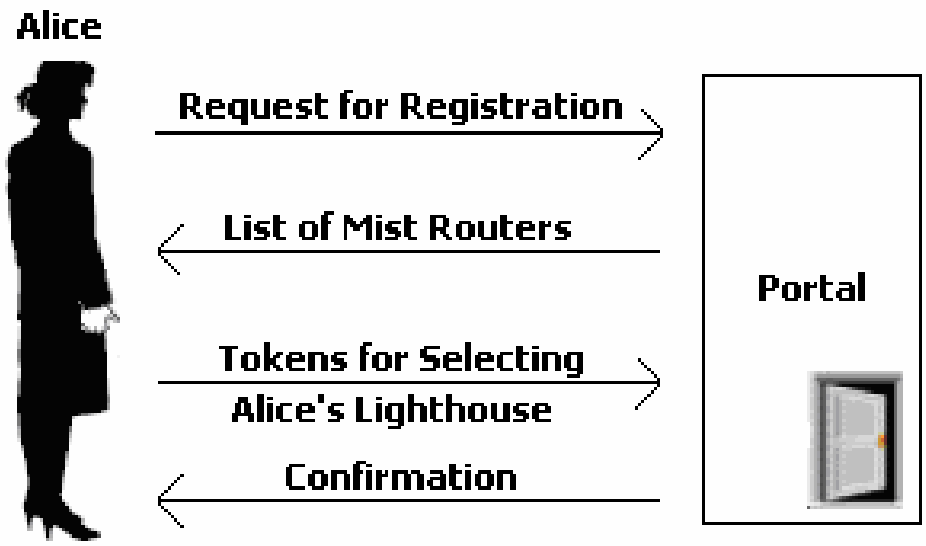
Best candidate: Mist

- Mist Communication
  - Hierarchy definition and initialization
  - Registration to Portal
  - Registration to Lighthouse
  - Mist circuit establishment
  - Data Exchange

Mist Hierarchies



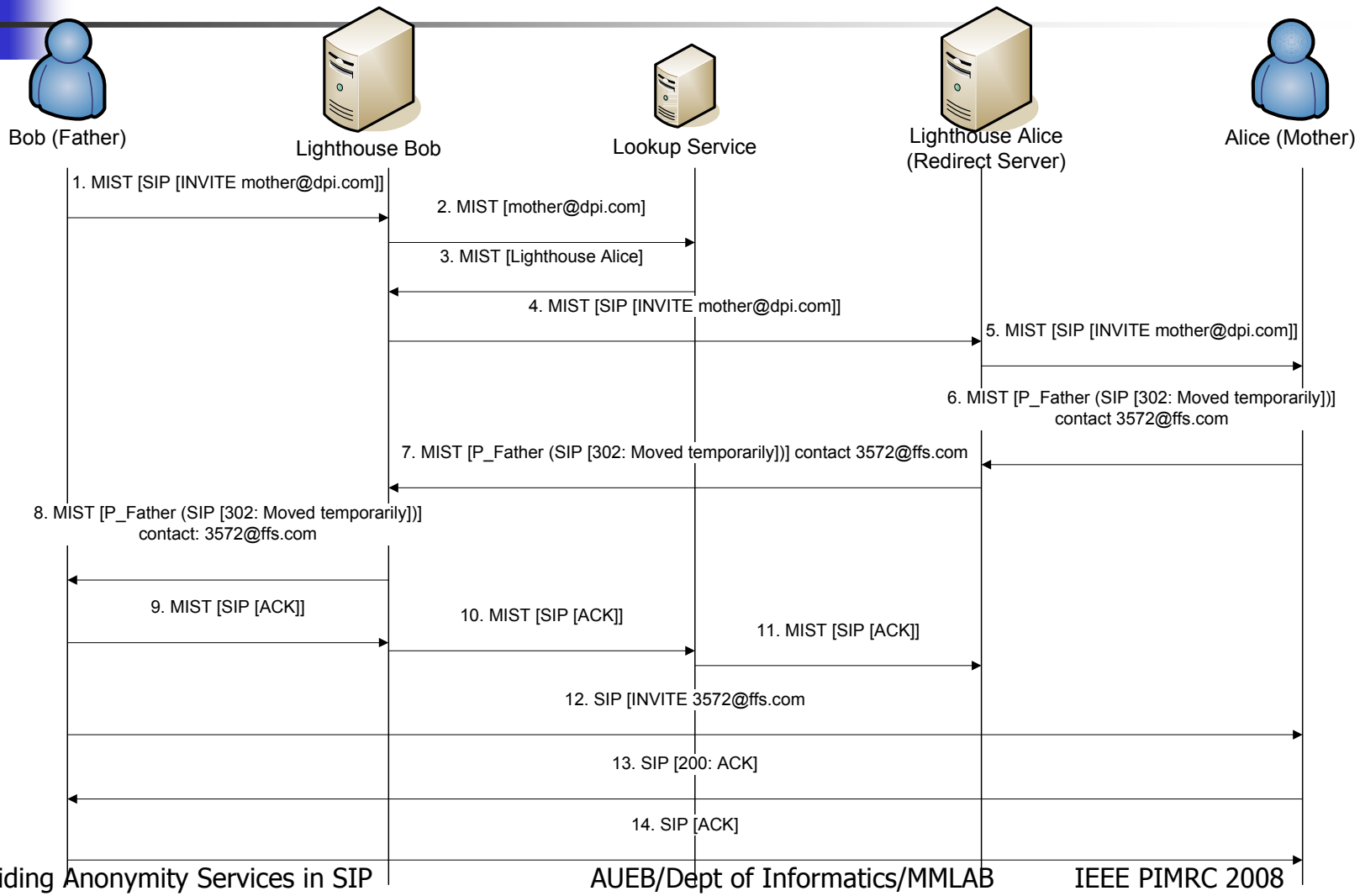
Mist Initialization

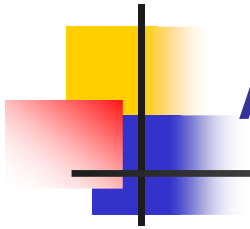


Applying Mist on SIP

- Assumptions:
  - SIP Home Server acts as Mist Lighthouse
  - SIP Remote servers act as Mist Portals
  - SIP location service instead of user's physical location will know the way to route packets to him.
  - Mist Hierarchy has been applied as overlay to the SIP Network
    - Add connections between the siblings of each level of the hierarchy

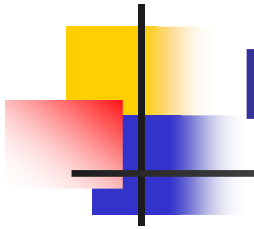
Establishing of a SIP Session through MIST





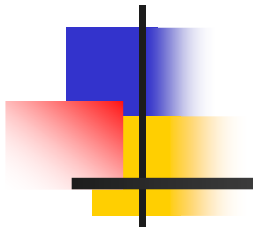
Advantages

- support untraceability of the packets routed through the Mist due to the distribution of knowledge (i.e., Portals know “where”, LIGs know “who”)
  - This preserves the privacy of the location of the users.
- For the users registered to the system using their nickname, assuming that the private keys have been issued based on this nickname:
  - anonymous communications are actually supported.



Further work

- Evaluate the proposal against privacy threats and vulnerabilities
- Measure anonymity
- Evaluate the proposal
  - Quantitative (delay, overhead, etc)
  - Real implementations under going
  - SIPp call generator
  - Soft clients



thank you

PIMRC 2008

Sept. 15, Cannes, France

L. Kazatzopoulos, K. Delakouridis, G.F. Marias

lkazatzo@aueb.gr, kodelak@aueb.gr, marias@aueb.gr