Information-Centric Networking & the Ψ Architecture

George C. Polyzos

Mobile Multimedia Laboratory
Department of Informatics
Athens University of Economics and Business
Athens, Greece

polyzos@aueb.gr
http://mm.aueb.gr/

Visiting Professor
CSE, UCSD

Office: CSE 3132
Tel.: 858 534 8615

polyzos@cs.ucsd.edu

ICN talk Outline

- Introduction, motivation, overview
- Research projects
- The Pub/Sub Internet (Ψ) Architecture
  - pub-sub, rendezvous
  - identifiers
  - forwarding
  - security aspects
  - testbeds and evaluation
- Discussion & Conclusion

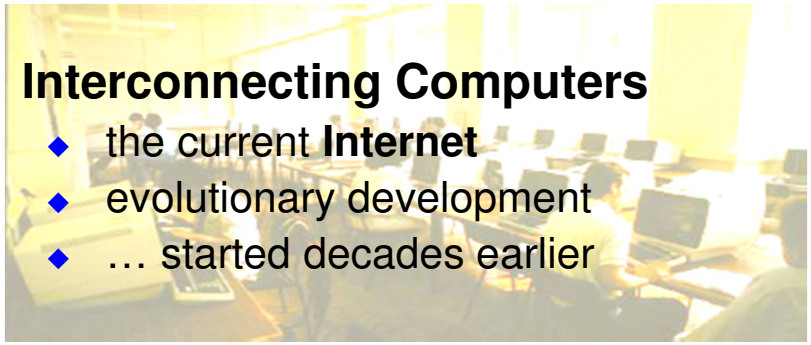
Mobile Multimedia Laboratory

History and Outlook

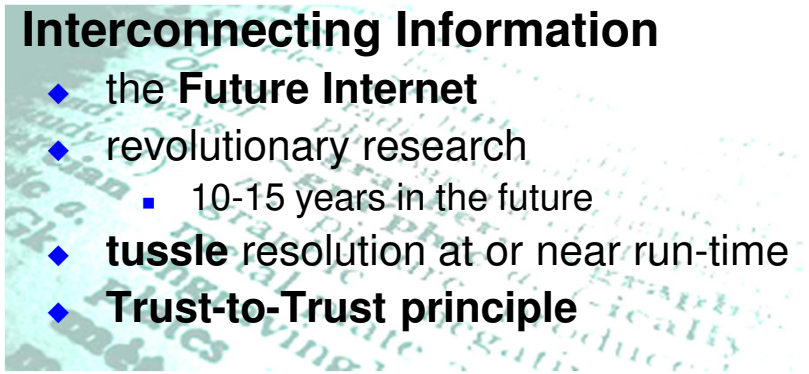
towards…
Information-Centric Networking

- At the **beginning**…
  - cooperation; no competition…
  - **no** commercial traffic!
  - endpoint-centric services/E2E
- **Now**…
  - Content distribution…
    - >50% of traffic today is video↑
  - Overlays… DPI by ISPs…
  - Trust? Endpoint trust?
    - viruses, phishing, DoS attacks…
  - E2E?
    - NAT, firewalls, middleboxes, CDNs
  - Current net economics favor sender
  - Tussles…
    - e.g.: privacy vs. accountability

- **Connecting Wires**
  - the past…



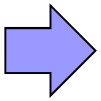
- **Interconnecting Computers**
  - the current **Internet**
  - evolutionary development
  - … started decades earlier



- **Interconnecting Information**
  - the **Future Internet**
  - revolutionary research
    - 10-15 years in the future
  - **tussle** resolution at or near run-time
  - **Trust-to-Trust principle**

Motivation for an Information-Oriented Architecture

- **End-to-end** communication **is not** the prevailing paradigm
  - Firewalls, NATs, proxy-servers…
- **Information-centric use** of the Internet
  - e.g. CDNs, proxy-servers
  - Overlay content delivery structures ignore
    - network topology & data location
    - Request aggregation hard to achieve without information-awareness!
- Imbalance of power in favor of the sender
  - The network will forward anything a sender will inject
- No trust
  - E.g., phishing, spam, viruses, worms, etc.
- No adequate support for mobility (& multicast)



It's the new ways the Internet is used, for which it was not designed…

Our ICN-related Research Projects

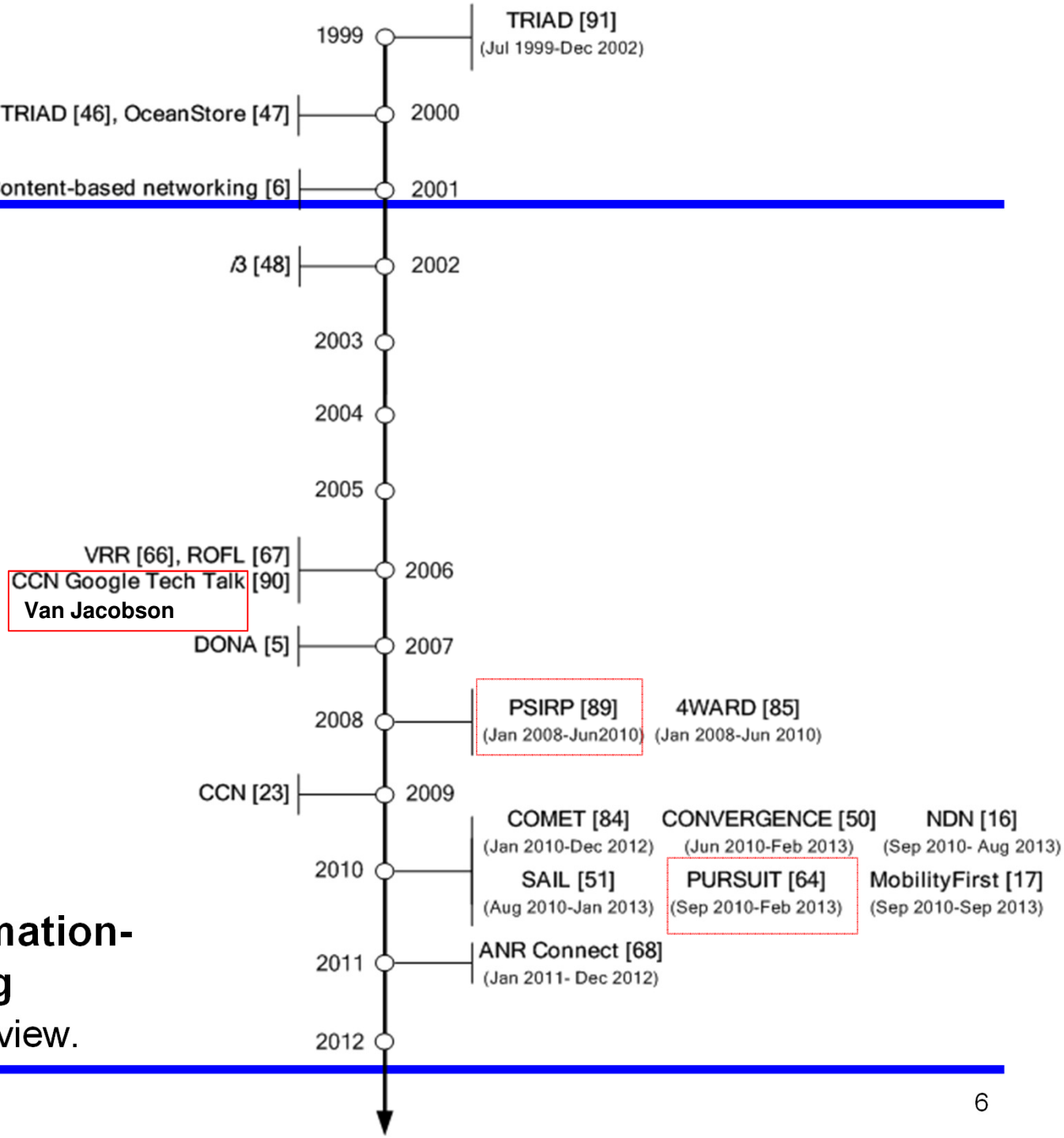
- **PSIRP**: Publish Subscribe Internet Routing Paradigm
  - FP7 ICT STREP, 2008-2010
    - the basis
    - focus on (inter)-networking

- **PURSUIT**: Publish Subscribe Internet Technologies
  - FP7 ICT STREP, 2010-2013
    - extending, above & below the Internet layer
    - optical, wireless, mobility, transport…

- **Euro-NF**: Anticipating the Network of the Future—From Theory to Design
  - FP7 ICT Network of Excellence, 2008-2012
    - ASPECTS, GOVPIMIT, E-key-nets

- **EIFFEL**: Evolved Internet Future For European Leadership
  - FP7 ICT SSA, 2008-2010; Think-Tank continued
  - June 2011 TT @ **MIT**: ***Information-Centric Networking***
- ***φSAT***: The Role of Satellites in Future Internet Services
  - European Space Agency funded
  - 2011-2013

ICN timeline



C.N. Ververidis,
V.A. Siris,
N. Fotiou,
X. Vasilakos,
C. Tsilopoulos,
K.V. Katsaros,
G. Xylomenos,
G.C. Polyzos,

"**A Survey of Information-Centric Networking Research**," under review.

ICN Research Community

- workshops…

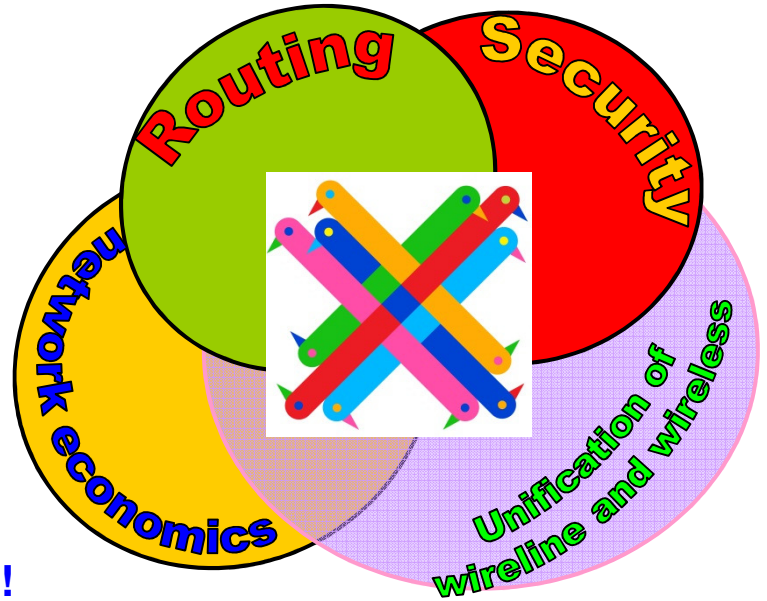
- ICN'11 w/ ACM SIGCOMM 2011 in Toronto
  - http://conferences.sigcomm.org/sigcomm/2011/workshops/ICN/

- ICN'12 w/ ACM SIGCOMM 2012
  - http://conferences.sigcomm.org/sigcomm/2012/icn.php

- Proposal for a 3rd ACM SIGCOMM WORKSHOP
  - ON INFORMATION CENTRIC NETWORKING
    - WITH ACM SIGCOMM 2013

Publish-Subscribe Internet Vision

- Envision a system that dynamically adapts to evolving concerns and needs of its participating users
  - **information centrism**
- Publish–subscribe based internetworking architecture restores the balance of network economics **incentives between the sender and the receiver**
- **Recursive use of publish-subscribe** paradigm enables dynamic change of roles between actors



Objectives

- Specify, implement and test an internetworked pub/sub architecture
  - follow a **clean-slate design** approach
- Perform qualitative and quantitative evaluation
  - **Security and socio-economics important!**
  - Migration and incentive scenarios important (e.g., overlay)!

The PSIRP Project

- EU FP7 ICT STREP, 2008-2010 (http://www.psirp.org/)

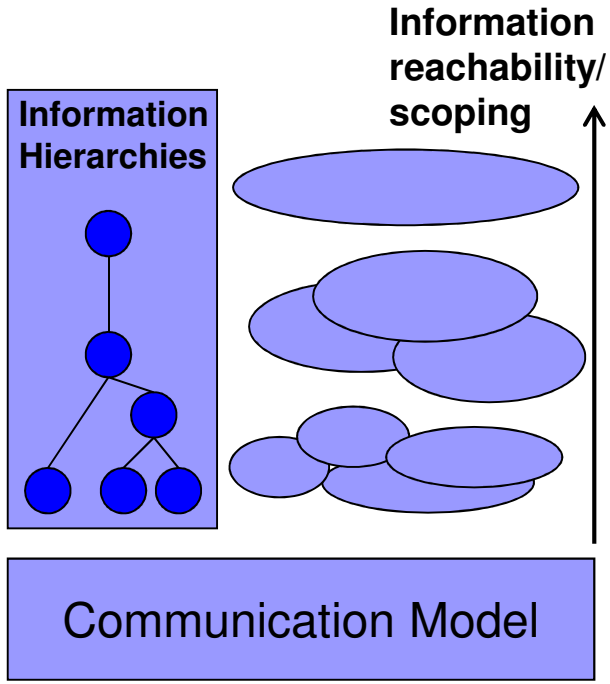
- A Pub/Sub based clean-slate architecture for the Future Internet
- Multicast (& caching) will be the norm
- Security (& privacy) are main design goals
- Mobility will be considered from the early stages of the design

- *Everything* is **Information**… (content, meta-data, publications…)
- Trust-to-Trust (T2T) principle

  - Helsinki Institute for Information Technology (HIIT)
  - RWTH Aachen
  - British Telecom (BT)
  - Oy LM Ericsson Ab (LMF)
  - Nokia Siemens Networks Oy (NSNF)
  - Athens University of Economics and Business (AUEB)
  - Institute for Parallel Processing, Bulgarian Academy of Science (IPP-BAS)
  - Ericsson Hungary Ltd. (ETH)

Main Design Principles of the Ψ Architecture

- Information is multi-hierarchically organised
  - Higher-level information semantics are constructed in the form of directed acyclic graphs (starting with e.g., ontologies).
- **Information scoping**
  - Mechanisms for limiting the reachability of information.
    - Physical
    - **Logical**
- Scoped information neutrality
  - Within each scope of information, data is only forwarded based on the given (scoped) identifier.
- **The architecture is receiver-driven**
  - No entity shall be delivered data unless it has agreed to receive those beforehand, through appropriate signalling.

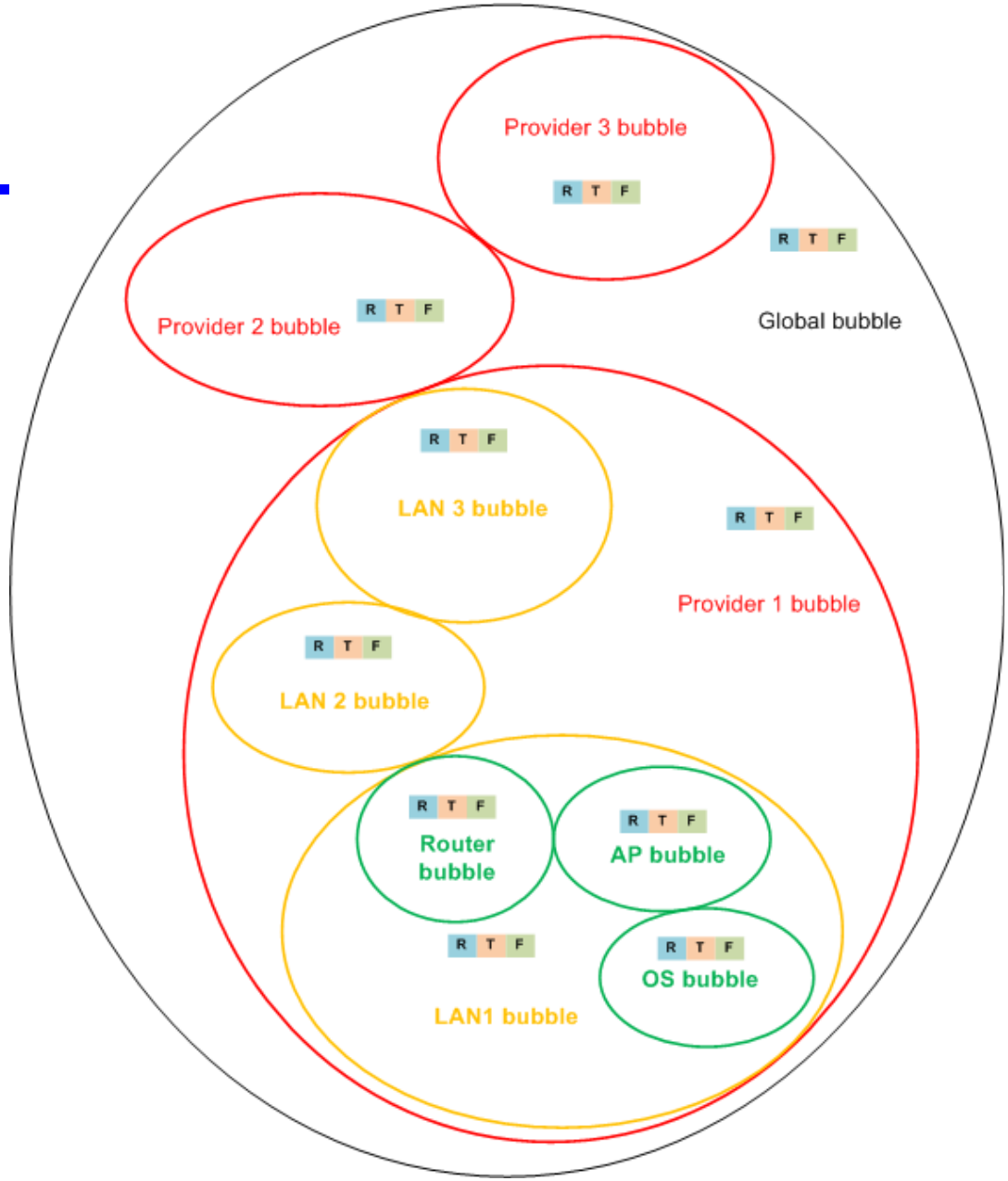


The PSI (Ψ) Architecture

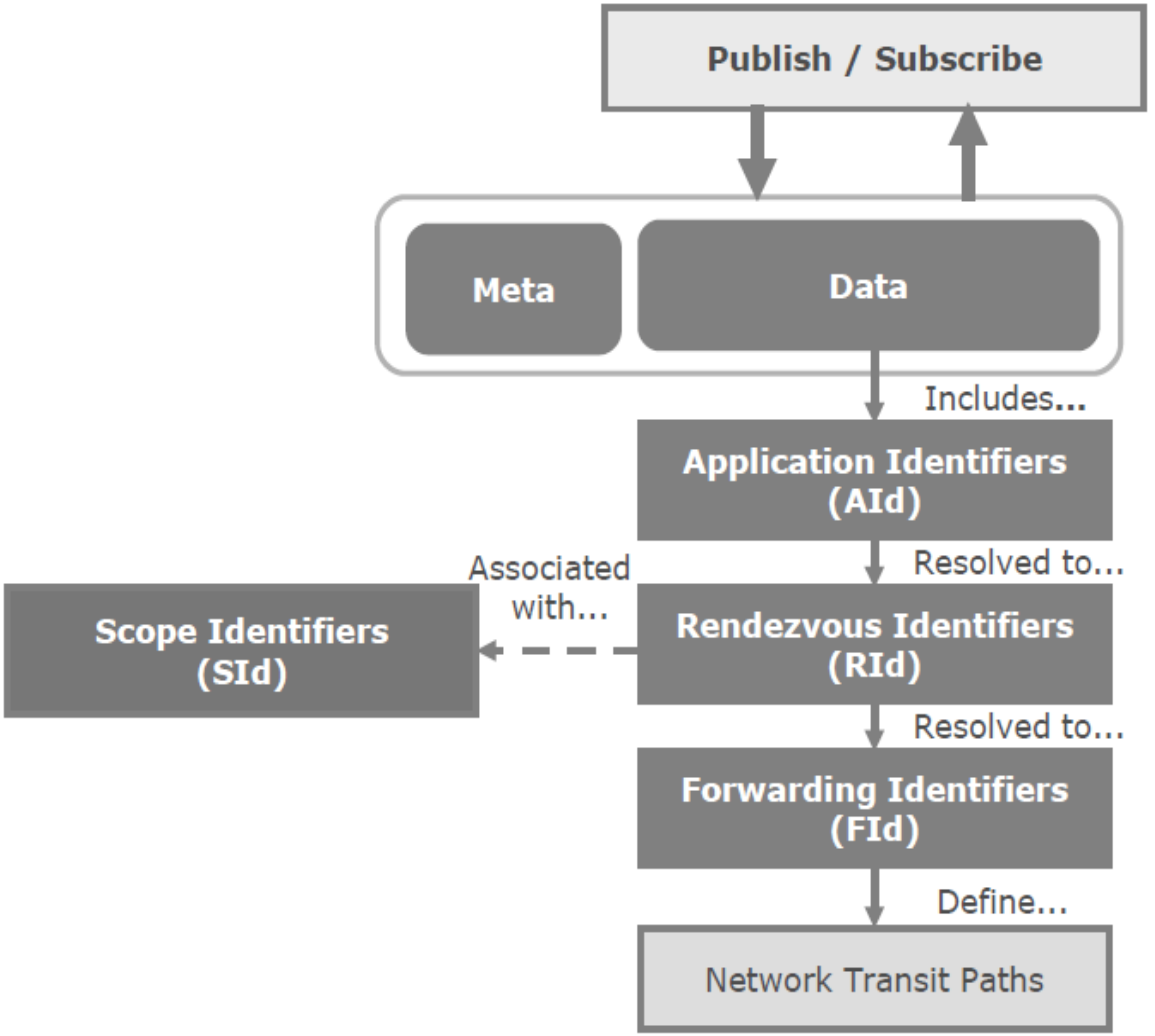
- Pub/Sub Internet Architecture
- Clean-Slate
- Native
- Two different prototype implementations exist
  - Blackhawk (PSIRP)
  - Blackadder (PURSUIT)

Basic Ψ Functions

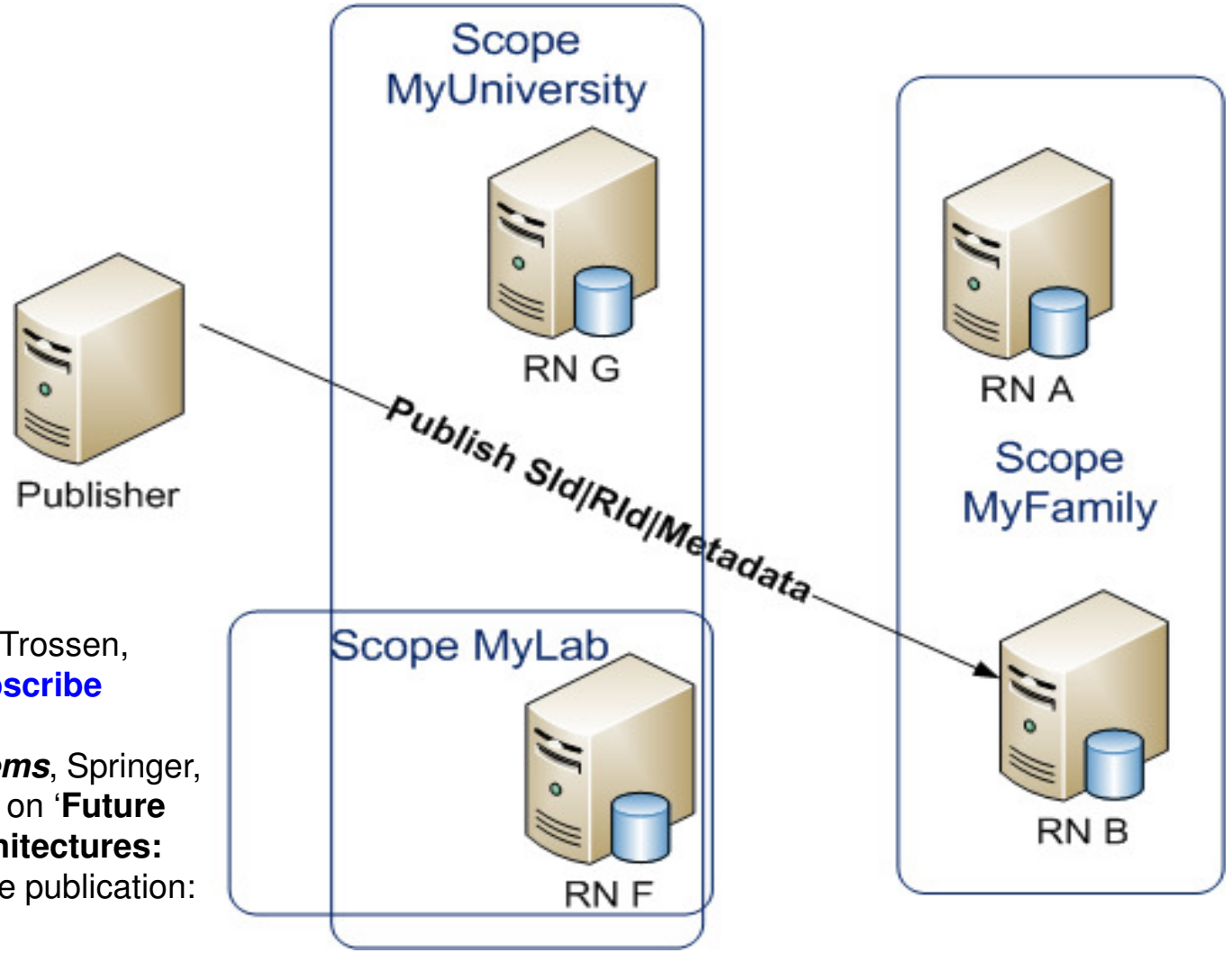
- Publications
  - Information/content
- Subscriptions (interests)
- ***R****endezvous*: Matches *publications* with *subscriptions* and initializes the forwarding process
- ***T****opology*: Monitors the network and it creates information delivery paths
- ***F****orwarding*: Implements information forwarding



Identifiers

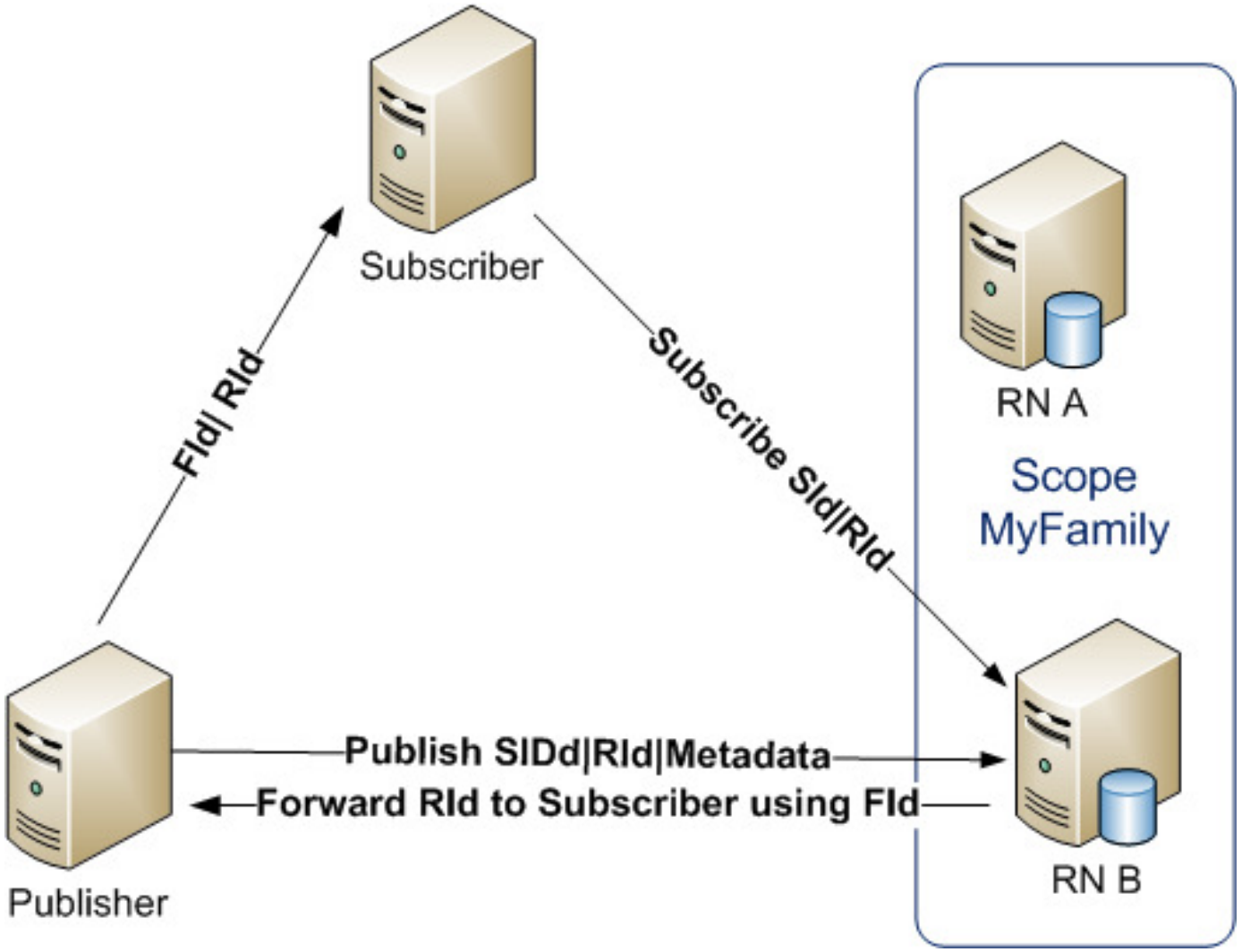


Ψ Publication

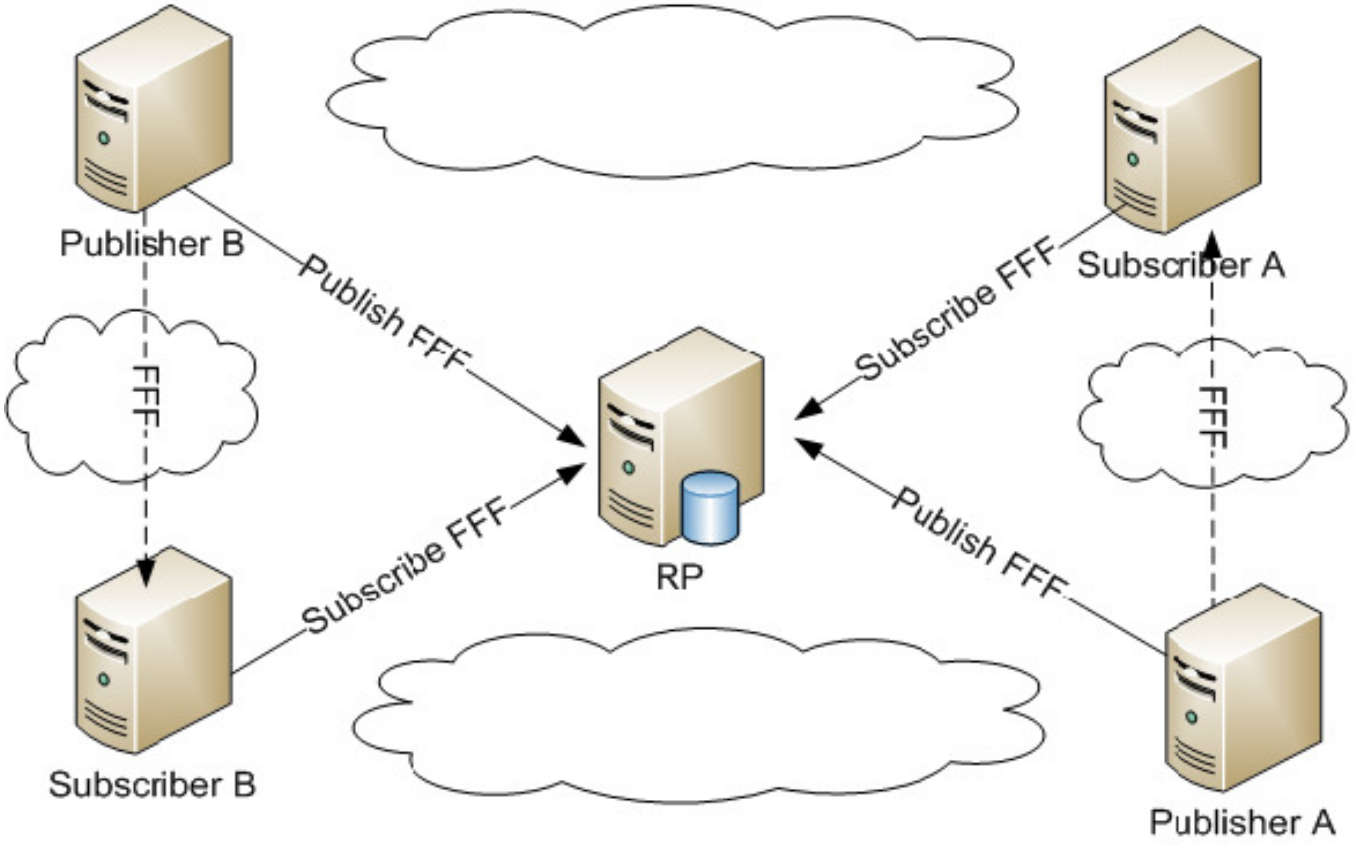


N. Fotiou, G.C. Polyzos, D. Trossen, "**Illustrating a Publish-Subscribe Internet Architecture**," ***Telecommunication Systems***, Springer, vol. 52, no. 3, Special Issue on '**Future Internet Services and Architectures: Trends and Visions**,' Online publication: 23/2/2011.

Ψ Subscription

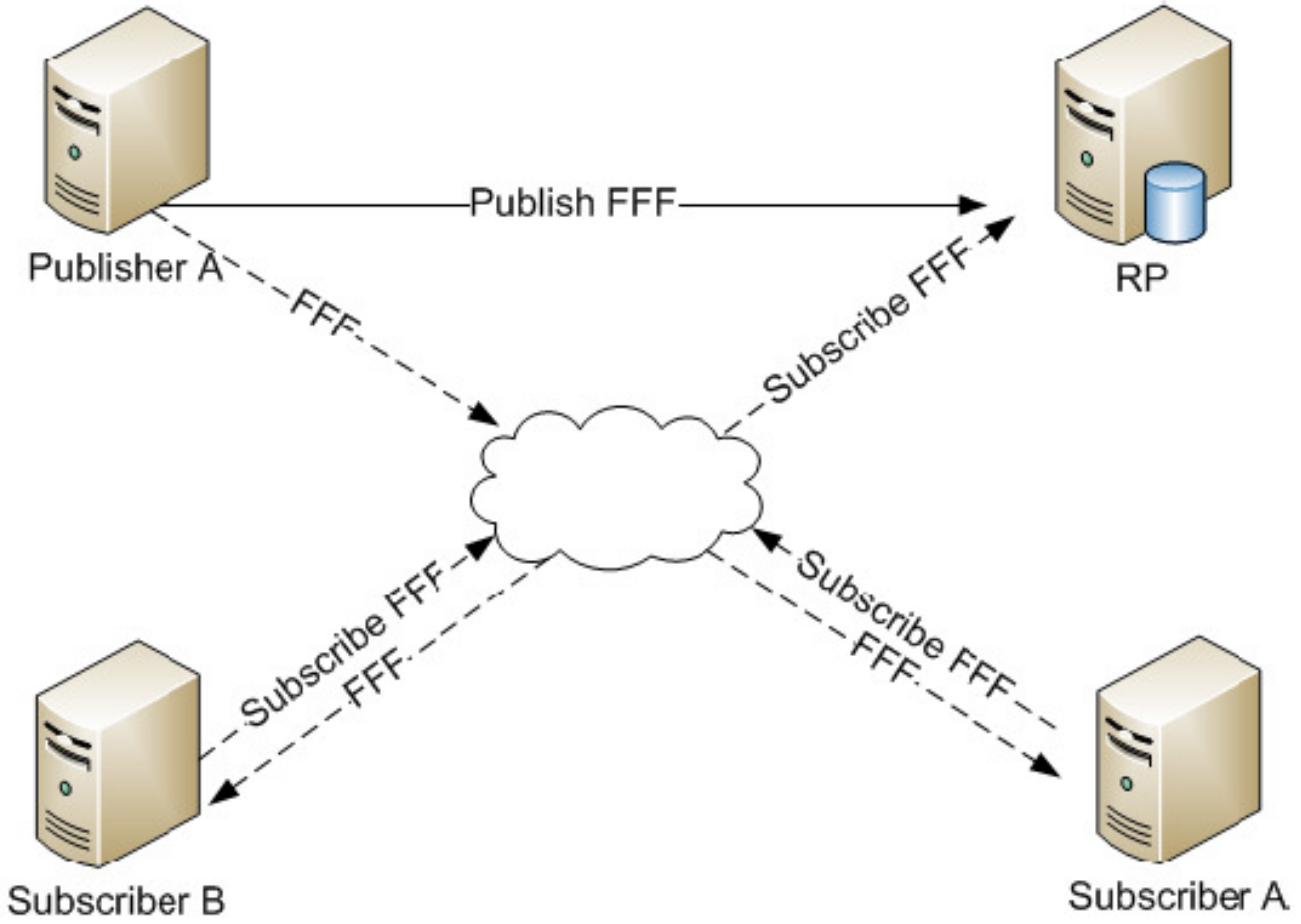


‘Caching’ or Multiple Information Providers & Multiple Paths



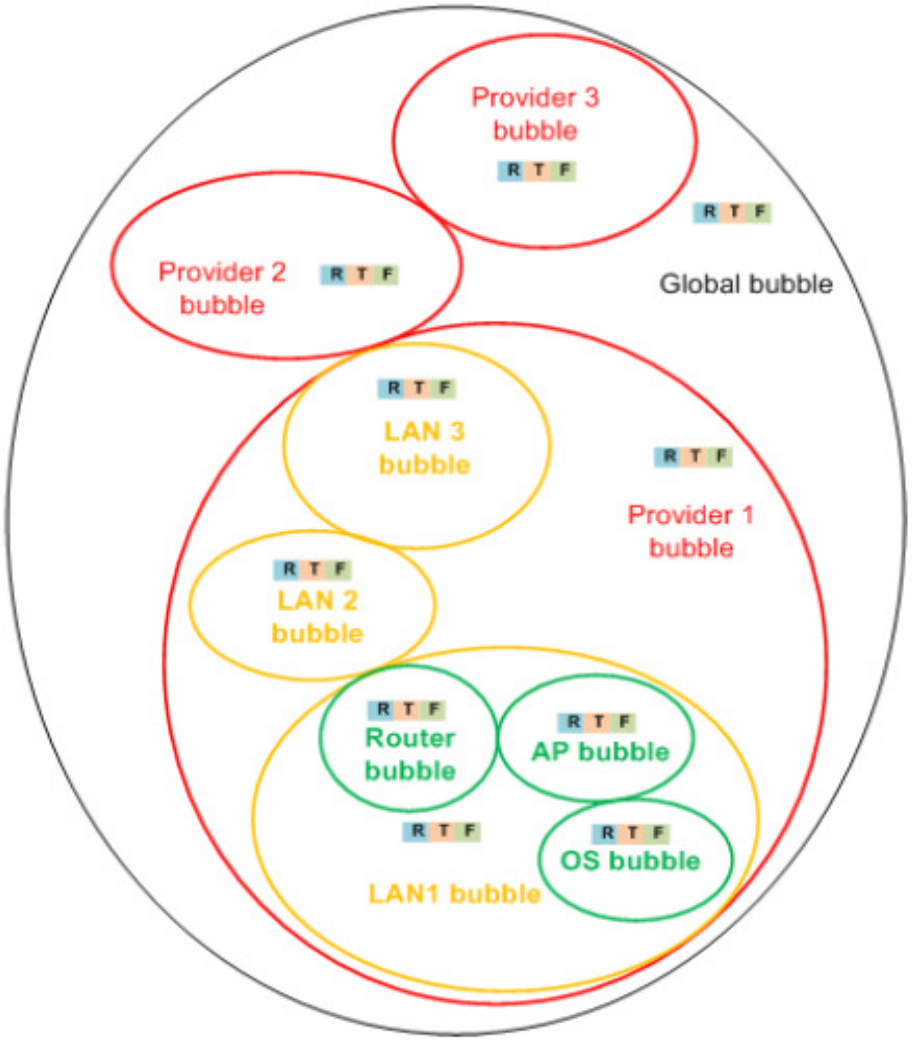
G. Xylomenos, et al., “**Caching and Mobility Support in a Publish-Subscribe Internet Architecture**,” ***IEEE Communications Magazine***, feature topic on ‘**Information-Centric Networking**,’ July 2012.

Resource Sharing / Multicast



Building Blocks in Ψ: *Bubbles*

- The ***bubble*** concept is akin to the current layering model
- The basic building block of functionality at all levels
  - from OS
  - through LAN
  - to Global Internetwork
- Bubbles offer availability and extensibility through the **recursive** execution of basic functions

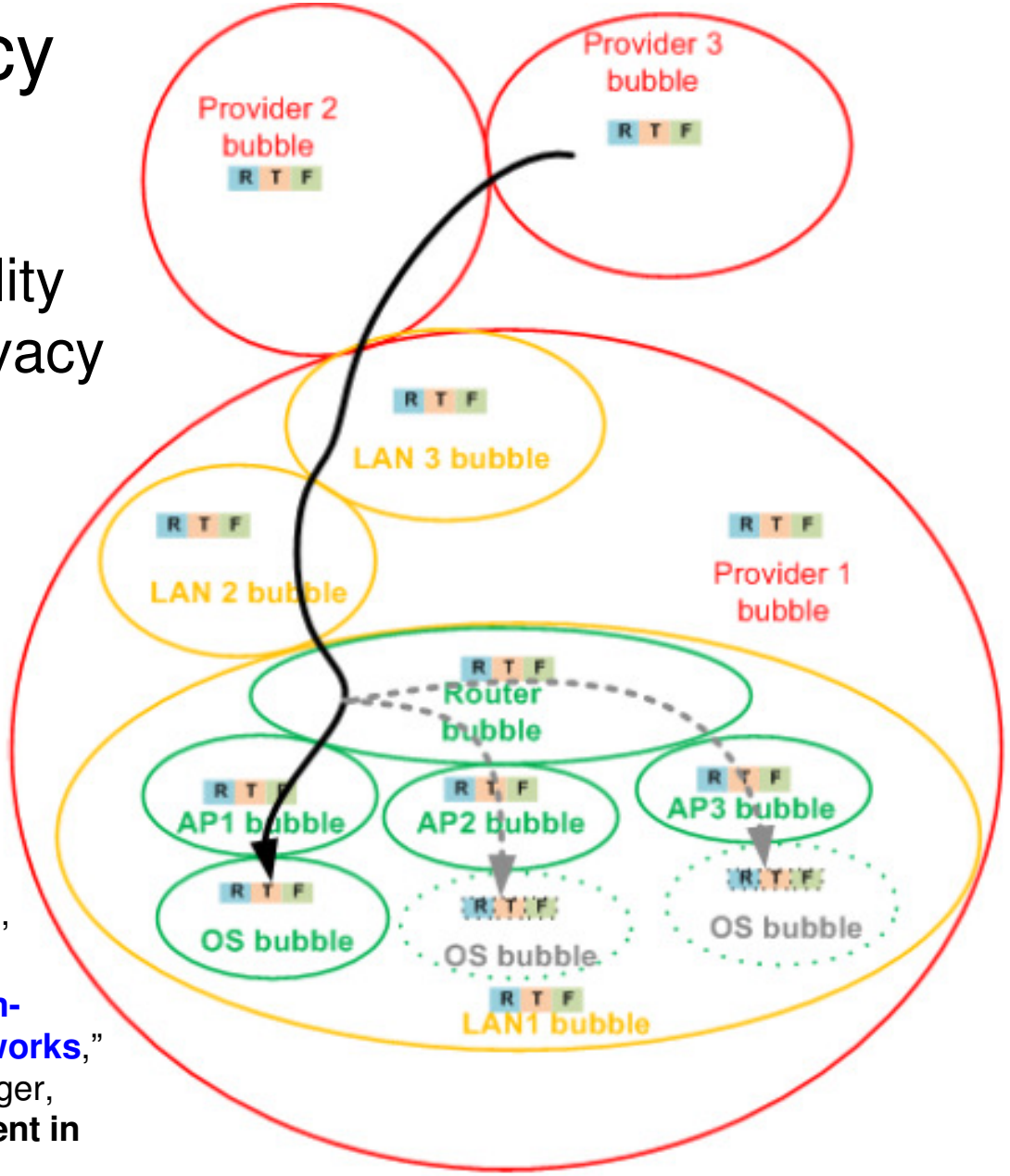


Bubbles...

- Need to implement the 3 basic functions:
  Rendezvous, *Topology* and *Forwarding* (RTF)
  - Rendezvous
    - responsible for matching subscriptions with publications
  - Topology
    - monitors the network topology
    - and creates information delivery paths
  - Forwarding
    - implements information forwarding
      … throughout the delivery path(s)
- ... differently, depending on level

Mobility and Privacy support

- Bubbles support mobility as well as location privacy



N. Fotiou, K.V. Katsaros G.C. Polyzos, M. Särelä, D. Trossen, G. Xylomenos, "**Handling Mobility in Future Publish-Subscribe Information-Centric Networks**," ***Telecommunication Systems***, Springer, Special Issue on '**Mobility Management in the Future Internet**,' to appear.

Security Requirements

- Publications confidentiality
  - publications should be not revealed to unauthorized subscribers
- Subscription confidentiality
  - user subscriptions should be kept secret
- Integrity, Availability
- Authentication, Anonymity
- Accountability
- Information Scoping

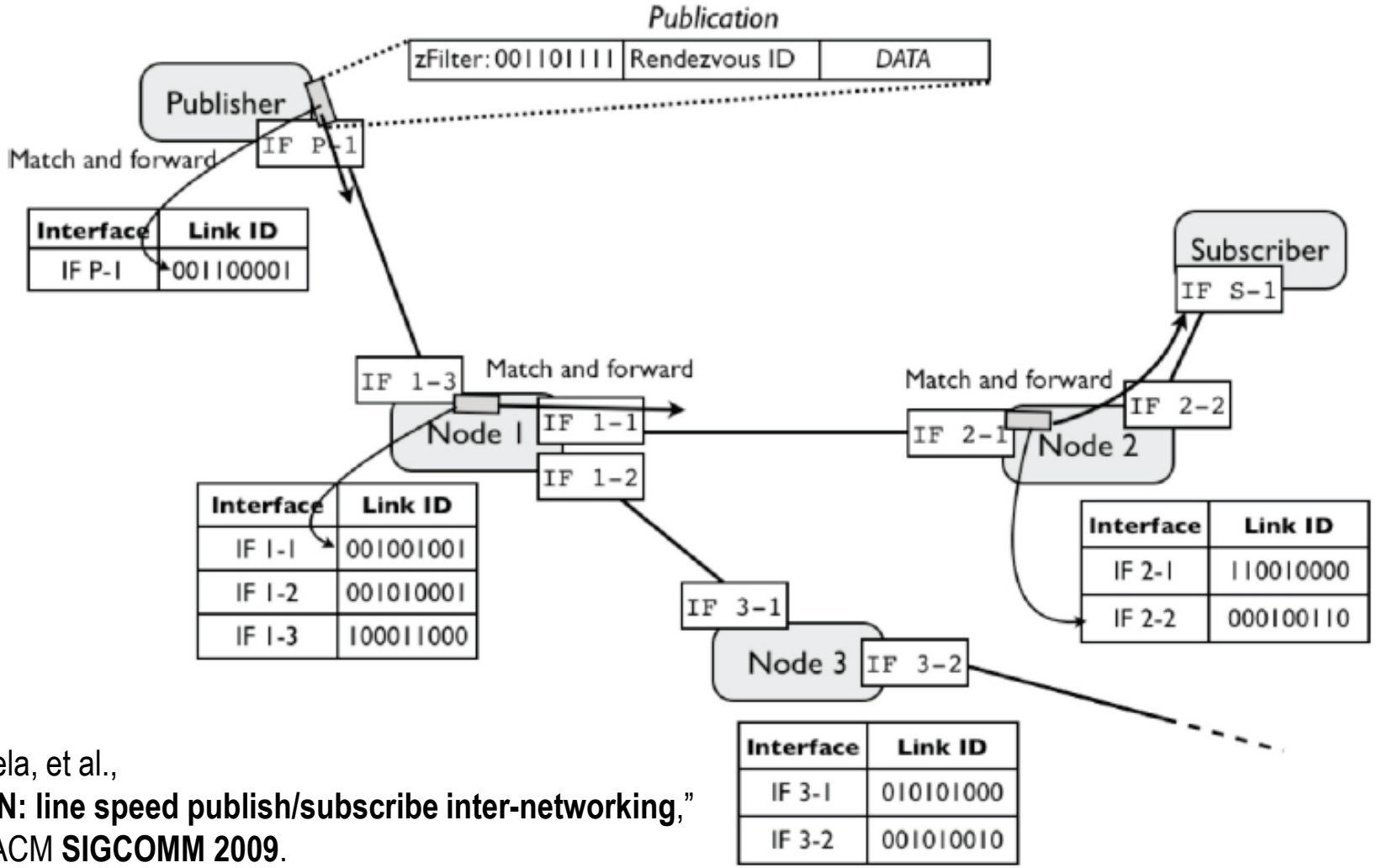
Scopes: Ψ's Information *Firewalls*

- Scopes allow for information location as well as for control of information dissemination
- Can be physical….
  - e.g., a sub-network
- … or logical
  - e.g., my friends in Facebook
- In scopes, access control and accounting mechanisms are/will be implemented

Secure Forwarding Mechanism

- Forwarding is based on the creation of a Bloom filter (called zFilter) that contains all the link identifiers through which a packet has to travel
- Link identifiers are unique per information flow
- zFilter creation involves an encryption mechanism
  - DoS attack resistant
  - Almost impossible to
    - redirect an information flow
    - send arbitrary packets to a destination

zFilters Based Forwarding



P. Jokela, et al.,
"**LIPSIN: line speed publish/subscribe inter-networking**,"
Proc. ACM **SIGCOMM 2009**.

Packet Level Authentication (PLA)

- Per packet public key cryptographic operations are possible
  - at wire speed
- The network carries only authentic data
  - Requires third-party certificates
- Need not be implemented at all nodes
  - Selected key nodes
- PLA offers significant energy efficiency
- Implemented in NetFPGAs

Security Characteristics of Ψ

- Pub/Sub restores the imbalance of power between sender and receiver(s)
- No information flow until **explicit** signal for
  - Interest for specific piece of information
    - Anti-Spam mechanism
  - Availability of a specific piece of information
    - Anti-DoS mechanism
- Pub/Sub facilitates
  - Anonymity
  - Mobility
  - Multihoming
- Message aggregation
  - Resource sharing (e.g., with multicast)

Security & Privacy

- E2E direct trust not applicable
  - Current Internet does not support it either
  - Socioeconomic trust through mediators (e.g., Rendezvous Providers)
    - D. Lagutin, K. Visala, A. Zahemszky, T. Burbridge, G.F. Marias, "**Roles and Security in a Publish/Subscribe Network Architecture**," Proc. IEEE ISCC 2010, Bologna, Italy, June 2010.
- Users change behavior, content does not
  - Rely on new methods to evaluate content integrity and authenticity
  - Reputable Content
    - N. Fotiou, G.F. Marias, G.C. Polyzos, "**Fighting Spam in Publish/Subscribe Networks Using Information Ranking**," Proc. 6th Conf. on Next Generation Internet (NGI), Paris, France, June 2010.
- End-user privacy can be effectively supported in ICN (at the internetwork level)
  - Who asks for what content hidden from content provider, caches
  - Pub/Sub matching through *trusted* mediator service (e.g., **Rendezvous** providers)
    - **BUT** privacy from Rendezvous providers becomes more of an issue
- Spam & malicious content distribution is blocked
  - There is no unsolicited traffic in the network!
    - Content is delivered after explicit request
  - New adversary models
    - P. Nikander, G.F. Marias, "**Towards Understanding Pure Publish/Subscribe Cryptographic Protocols**," Cambridge Security Protocols Workshop (SPW), June 2008 .

Advantages of PSI in Mobility Support

- Publishers & Subscribers can seamlessly & simultaneously move
  - Data (packets) are identified independently from source or destination
  - Information (cached? content) is still transparently available
- Publish/Subscribe is **asynchronous** and **multicast**
  - Adapts better to frequent mobility
- Routing and Forwarding
  - decoupling IDs from location is a major advantage
    - locations are ephemeral
    - no need for **triangular** routing
    - **ingress filtering** problem
    - **anycast** choice of the best source of content

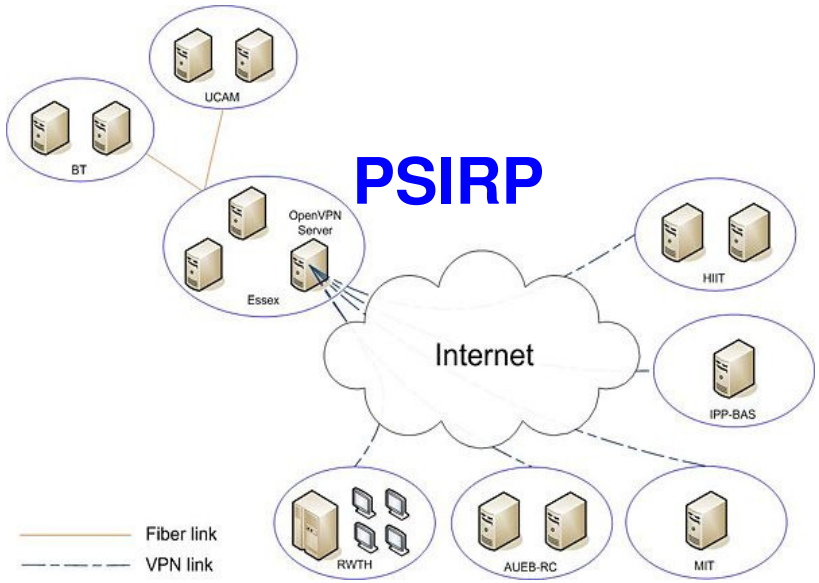
The PURSUIT Project

- EU FP7 ICT STREP, 2010-2013 (http://www.fp7-pursuit.eu/)

- *information-centric* view on networking
- Focusing on *WHAT* is being exchanged
  - rather than who are exchanging it, or where it is
- Builds on the results of PSIRP
- Designing (/extending/completing) an internet architecture based on pub/sub
  - Routing
  - Security
  - Economics
  - Unification of Wireless w/ Wireline

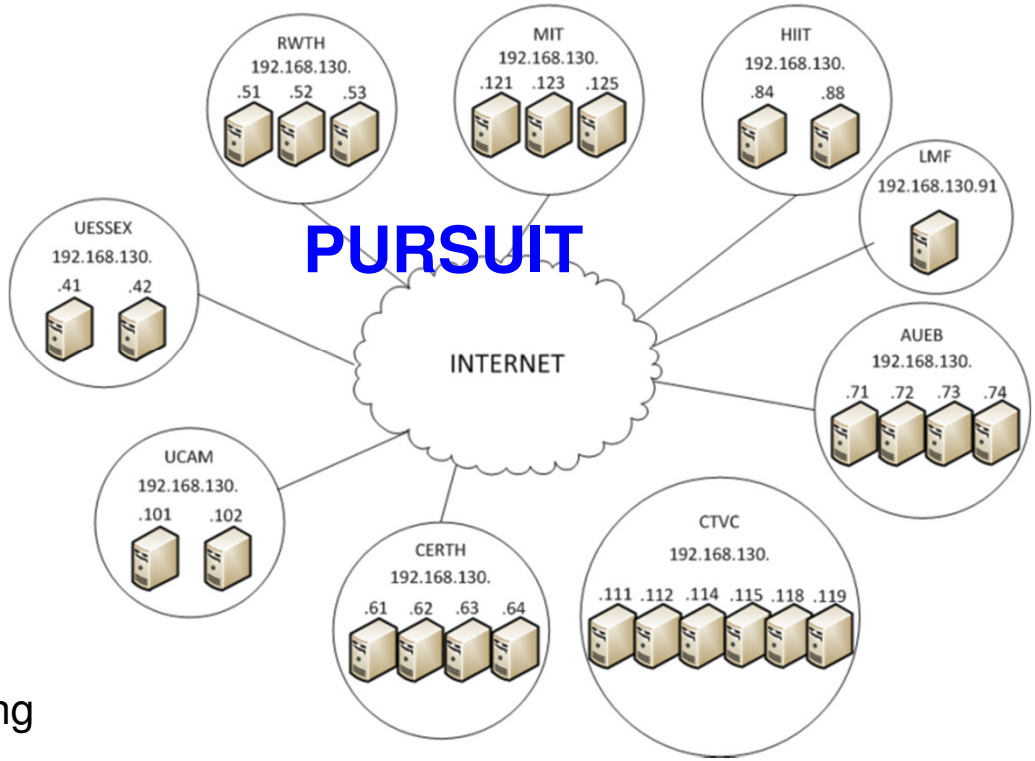
- 8 partners from 4 EU countries: Finland, Germany, Greece and UK
  - Aalto University (FI)
  - RWTH Aachen University (DE)
  - Athens University of Economics and Business (GR)
  - University of Cambridge (UK)
  - Oy L M Ericsson Ab (FI)
  - Centre for Research and Technology Hellas (GR)
  - University of Essex (UK)
  - CTVC Ltd (GB)

Prototype Implementations & Testbeds



PSIRP Testbed (w/ Blackhawk)
- 6 countries: UK, FI, GR, D, BU, **US**
  - In addition: Belgium during ICT demos
- Tunneled over the public Internet
  - +**dedicated fiber** where available

PURSUIT Testbed (w/ Blackadder)
- 25 nodes
- 5 countries: UK, FI, GR, D, **US**
- Tunneled (VPN)
  - over the public Internet

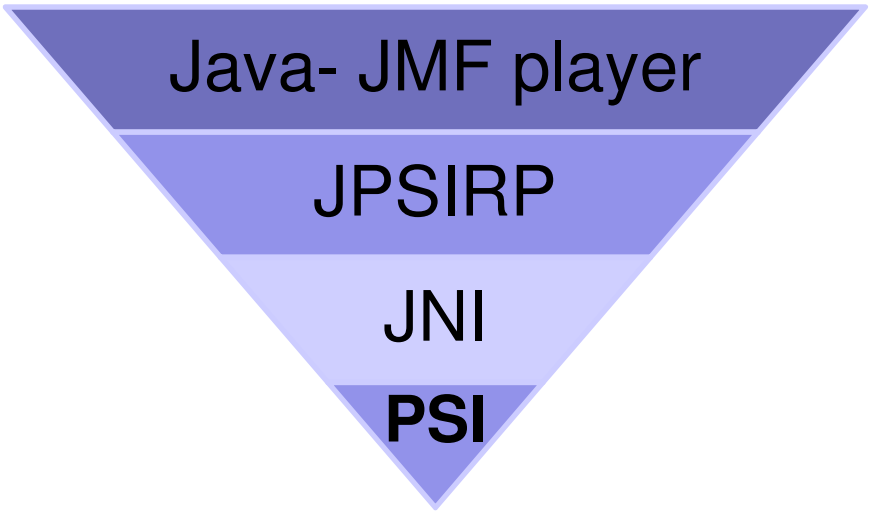


Current & future work
- multipath transport, multimedia streaming
- Wireless/mobile testbed extensions

Multimedia over Ψ

- Motive: Multimedia over Ψ
  - “YouTube” a la Ψ …
- Streaming videos
  - without RTP/TCP/IP
  - only native Ψ
- Basic Components of the application:
  - **Publisher**: the owner of the video
  - **Subscriber**: the user that seeks to view the video

- Technologies Involved



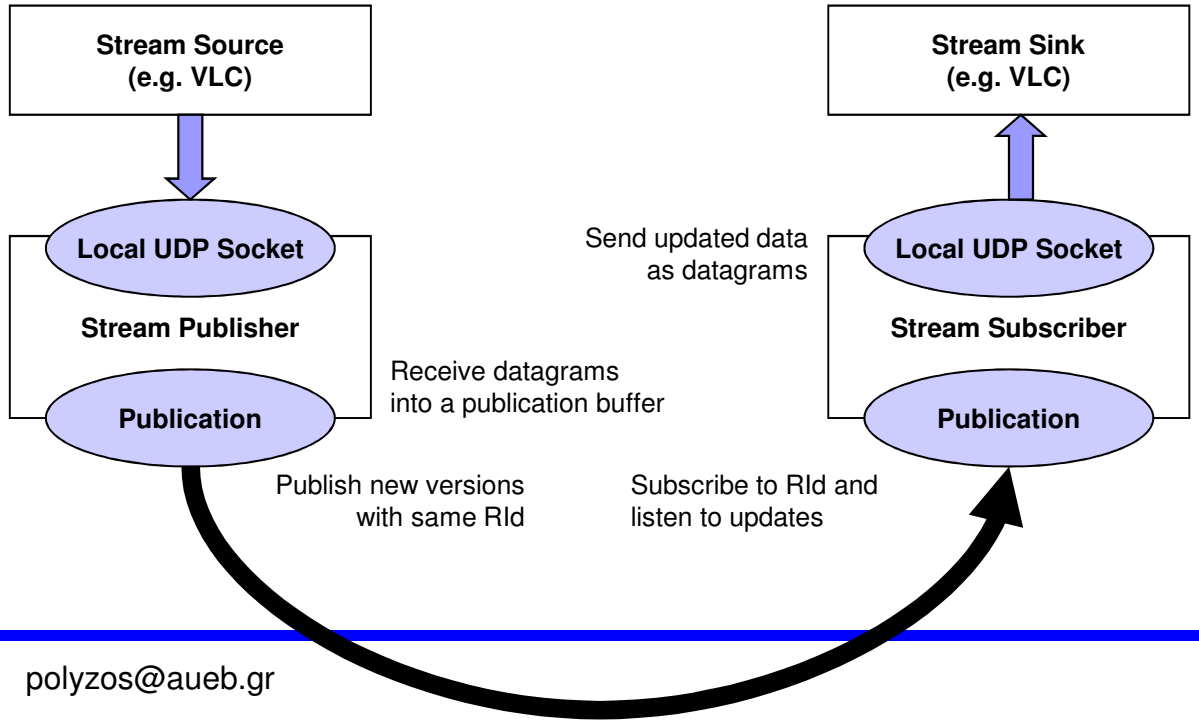
- We tried different applications
  - Video
  - Audio/voice (VoPSI)
  - ...

Publish Videos

- Publish a video or a directory with multiple videos
- Define the scope for the video she uploads to the network
- Currently done via local exchange of video knowledge

Subscribe to a Video

- Search for the desirable video using the name of the video
  - Currently done via local exchange of information
- Subscribe to its PSI-level identifiers
- Play the video while downloading



NOTE: The publisher knows the subscriber set for this RId, sends the metadata directly to the subscribers; no rendezvous. Subscriber with metadata for a new version, subscribes to the corresponding data chunks.

An Information-Centric Overlay Network Architecture for Content Distribution and Mobility Support

Ph.D. Dissertation by Konstantinos Katsaros

- **Multicast**
  - *Router Assisted Overlay Multicast (RAOM)*
    - Deploying multicast functionality in an overlay fashion
- **Multicast & Caching**
  - *MultiCache*
    - Enabling caching of data delivered by multicast trees
- **Adapting to the inter-network structure**
  - *H-Pastry*
    - Canonical version of Pastry
- **Mobility Support**
  - *Overlay Multicast Assisted Mobility (OMAM)*
    - Revisiting multicast assisted mobility

K.V. Katsaros, G. Xylomenos, and G.C. Polyzos, "**MultiCache: an Overlay Architecture for Information-Centric Networking**," ***Computer Networks***, vol. 55, no. 4, pp. 936-947, Elsevier, Special Issue on 'Architectures and Protocols for the Future Internet,'March 2011.

Conclusions

- ICN is well positioned to address
  - mobility, caching, security...
  - evolution: **tussles resolved at or near run-time**
- The Ψ architecture inherits the advantages of
  - **ICN** & the **publish/subscribe** paradigm
  - in particular the security ones, but….
- PSI(RP) selected and added specific security mechanisms
  - Secure Forwarding (zFilters)
  - Scopes
  - Bubbles
  - Packet Level Authentication
  - Information ranking

PSI: Key Observations and Issues

- RIDs: hash of content vs. not...
  - Implications of uniquely indentifying content
    - Caching (enabled/facilitated)
- SIDs as special case of RIDs
- pub/sub “recursively”
  - at many levels of the hierarchy/network
    - from wire-level to the global Internet
    - perhaps used to realize reliable transport
- Granularity of items (to publish/subscribe to)
- pub/sub model: documents vs. channels
  - versions (& IDs) of publications?
- Algorithmic Identifiers (RIDs)
  - nice for intra-channel IDs...
- asynchronous (subscribe before publish)
- search engines probably still important (at different level?)
- Naming vs. IDs?
- Mobility, multi-homing, soft handoff...

More Observations, Questions & Issues

- information vs. content-centric vs. named data vs. pub/sub vs. ...
- overlay vs. clean-slate
  - special-purpose nets only? Not global?
- Wireless?
- Rendezvous
  - powerful
  - trusted
    - has lots of information...
  - target of DOS attacks
  - networks of RPs = RN
  - belongs to different entities than network provider?
  - competing RN
  - RP functionality needed at multiple & different levels
    - Intranet, global... on a wire...

Thank you!

Information-Centric Networking & the Ψ Architecture

George C. Polyzos

Mobile Multimedia Laboratory
Department of Informatics
Athens University of Economics and Business
Athens, Greece

polyzos@aueb.gr
http://mm.aueb.gr/

Visiting Professor
Dept. of Computer Science & Engineering
University of California, San Diego

Office: CSE 3132
Tel.: 858 534 8615

polyzos@cs.ucsd.edu