Information-Centric Networking & the $\Psi$ Architecture

George C. Polyzos

Mobile Multimedia Laboratory
Department of Informatics
Athens University of Economics & Business
Athens, Greece
polyzos@aueb.gr
http://mm.aueb.gr/

Dept. of Computer Science & Engineering
University of California, San Diego
polyzos@cs.ucsd.edu
http://cs.ucsd.edu/~polyzos/
ICN talk Outline

- Introduction, motivation, overview
- The Pub/Sub Internet (Ψ) Architecture
  - pub-sub, rendezvous
  - identifiers
  - forwarding/LIPSIN
  - prototypes, testbeds, and evaluation
- Security aspects
- Mobility support
- Continuous Media/Multimedia
- The role of Satellites
- Discussion & Conclusion
Internet History and Outlook

- **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
  - The sender has the power...
  - Tussles...
    - e.g.: privacy vs. accountability

---

towards...
Information-Centric Networking

- **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

polyzos@aueb.gr
Publish-Subscribe Internet Vision

- **information centrism**
  - everything is information & information is everything
- **Recursive** & and generalized use of publish-subscribe
  - enables dynamic change of roles between actors
  - Network cache
    - publishes info (cached)
    - subscribes to get info to cache
  - Access Points publish ID
    - mobiles subscribe

**Objectives**
- Specify, implement, & 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)!

polyzos@aueb.gr
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

papers/talks

projects

“A Survey of Information-Centric Networking Research,” forthcoming
ICN Research Community

- workshops…
  - with ACM SIGCOMM
    - ICN 2011 (Toronto)
    - ICN 2012 (Helsinki)
    - ICN 2013 (Hong Kong):
      - 3rd ACM SIGCOMM ICN workshop
        - Abstract: March 10
        - Paper: March 17
  - with IEEE INFOCOM
    - NOMEN 2012
    - NOMEN 2013
- ICNRG@IERTF
- Journal & Magazines Special Issues

polyzos@aueb.gr
The PSI (Ψ) Architecture

- Pub/Sub Internet Architecture
- Clean-Slate
- Native

- Two different prototype implementations exist
  - Blackhawk (PSIRP)
  - Blackadder (PURSUIT)
Basic PSI Functions

- Publications
  - information/content
  - metadata
- Subscriptions (interests)
- **asynchronous** & in any order
- **Rendezvous**: Matches publications with subscriptions & initializes the forwarding process
- **Topology**: Monitors the network and it creates information delivery paths
- **Forwarding**: Implements information forwarding

polyzos@aueb.gr
Identifiers

- Publish / Subscribe
- Meta
- Data
- Application Identifiers (AId)
- Rendezvous Identifiers (RId)
- Forwarding Identifiers (FId)
- Network Transit Paths

Scope Identifiers (SID)

polyzos@aueb.gr
Subscription
‘Caching’ or Multiple Information Providers & Multiple Paths

Resource Sharing / Multicast

Publisher A

Publish FFF

RP

Subscribe FFF

Subscriber B

Subscriber A

polyzos@aueb.gr
Building Blocks in Ψ: Bubbles

- Needed to implement the 3 basic functions: *Rendezvous, Topology & Forwarding* (RTF)

- 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

polyzos@aueb.gr
Secure Forwarding Mechanism

- Forwarding based on Bloom filter (called zFilter) that contains all the link IDs through which a packet has to travel
- Supports multicast
- Hashing
  - False positives
  - Limitations in size
    - Hierarchical / inter-networks
- 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


polyzos@aueb.gr
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

Caching and replication

- All content sources are equivalent in PSI
  - Origin, cache, or replication point
  - Chunks can be retrieved from different sources
  - Sources are visible to the network
  - Network-level caching

- Caching vs. replication
  - Similar to the user, different to the network
  - Replication is planned (as in CDNs)
  - Caching is opportunistic (as in P2Ps)
  - PSI handles both in a unified manner
On-path caching

- **Very lightweight**
  - bypasses rendezvous network

- **Good for**
  - multicast error control
Off-path caching

- Uses the rendezvous network
  - to serve more users
- Good for
  - local (access network) caching
Content replication

- The rendezvous network chooses the best source
- Good for CDN-like proactive replication

polyzos@aueb.gr
Security Requirements

- Publications confidentiality
  - publications should not be 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

polyzos@aueb.gr
Access Control Enforcement Delegation

- **Motivation**
  - Kazaa: 50% of versions and copies **polluted** [INFOCOM’05, Liang et al.]
  - Kazaa: 15% infected by **52 different viruses** [SIGCOMM06, Shin et al.]
  - Limewire: 68% of executables, archives is **malware** [SIGCOMM’06, Kalafut et al.]

- **Observations**
  - users can change behavior, information cannot!
  - Information identification is easier
    - Hash function vs. Certificates

- **Design**
  - only positive, implicit votes
    - only 1 vote per item/publisher
    - no communication overhead
  - weight of a vote:
    - \( 1/\left( \sum \text{votes of pub in this set} \right)^{\alpha} \)

---


polyzos@aueb.gr
Information Identification

Prefix
- May give a location hint, denote the principal/owner
- Associated with an access control policy
- Handled by a (set of) dedicated network node(s)

Suffix
- Identifies uniquely the information object (globally or within the prefix)

- Users can create prefix, advertise prefix/suffix pairs, request prefix/suffix pairs

facebook.com/nikos/pics/ IMG32010234

prefix Suffix
PSI Implementation

- Prefix: Scope Identifier (SId)
- Suffix: Rendezvous Identifier (RId)
- SIds are managed by the Rendezvous node

- Users can advertise data and subscribe to data
- Information flow:
  - Define access control policy: who can advertise, who can subscribe
  - A subscriber has properly authenticated himself and requests item X
  - Provide Credentials
  - Subscribe Item (SId/RId)
  - Notify
  - Advertise Item (Sid/RId)
  - Create Scope (SId)
  - Publish Data
  - Owner (Publisher)
  - Consumer (Subscriber)
Benefits

- Consumer credentials protected
- Minimum user intervention
- RP has no access to consumer’s personal information
- RP does not have to implement any access control policy
- Access control policies can be re-used
  - Even by users who do not know their content
  - “Access Control Store”
- Access control policies can be easily modified
Mobility and Privacy support

- Bubbles support mobility as well as location privacy


polyzos@aueb.gr
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)

polyzos@aueb.gr
InfoRanking: lightweight mechanism to distinguish and isolate polluted information

- **Motivation**
  - Kazaa: **50%** of versions and copies polluted [INFOCOM’05, Liang et al.]
  - Kazaa: **15%** infected by **52 different viruses** [SIGCOMM06, Shin et al.]
  - Limewire: **68%** of executables, archives is malware [SIGCOMM’06, Kalafut et al.]

- **Observations**
  - users can change behavior, information cannot!
  - Information identification is easier
    - Hash function vs. Certificates

- **Design**
  - only positive, implicit votes
    - only 1 vote/item/publisher
    - no communication overhead
  - weight of a vote:
    - \( \frac{1}{\left( \sum \text{votes of pub in this set} \right)^{\alpha}} \)

Security & Privacy

- **E2E direct trust not applicable**
  - Current Internet does not support it either
  - Socioeconomic trust through mediators (e.g., Rendezvous Providers)

- **Users change behavior, content does not**
  - Rely on new methods to evaluate content integrity and authenticity
  - Reputable Content

- **End-user privacy can be effectively supported in ICN (@ 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
Advantages of PSI in Mobility Support

- Decoupling IDs from location
  - Publish/Subscribe is **asynchronous** and **multicast**
    - Adapts better to frequent mobility
- Publishers & Subscribers can seamlessly & simultaneously move
  - Data (packets) are identified independently from source or destination
  - Information (cached? content) is still transparently available
- 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
- Mobility & user behavior prediction together with proactive **caching/prefetching** can be used to enhance mobility support

G. Xylomenos et al., “**Caching and Mobility Support in a Publish-Subscribe Internet Architecture,**” *IEEE Communications Magazine*, July 2012.
Proactive Selective Neighbor Caching for enhancing Mobility Support in ICN

**Mobility**
- Delay can be reduced by using proxies to pre-fetch and cache data
  - approaches
    - Reactive
    - Durable subscriptions
    - Proactive
  - **Proactive Selective Neighbor Caching**
    - mobile initially connected to proxy i
    - select an optimum subset of neighbor proxies
      - i will send the mobile’s subscriptions, and
      - which will proactively cache
        - information items matching these subscriptions
    - if the mobile connects to one of these proxies
    - then it can immediately receive information items
    - it did not receive due to its disconnection

**Cost Function:**

\[
P_{\text{hit}}(S) \cdot C_{\text{hit}} + (1 - P_{\text{hit}}(S)) \cdot C_{\text{miss}} + N(S) \cdot C_{\text{cache}}
\]

Multimedia over $\Psi$

- Motive: Multimedia over $\Psi$
  - “YouTube” a la $\Psi$ ...

- Streaming videos
  - without RTP/TCP/IP
  - only native $\Psi$

- Basic Components of the application:
  - **Publisher**: the owner of the video
  - **Subscriber**: the user that seeks to view the video

- Technologies Involved
  - Java- JMF player
  - JPSIRP
  - JNI
  - PSI

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

polyzos@aueb.gr
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.

polyzos@aueb.gr
Optimization of Real-Time Media Distribution

Exploit
1. Functional organization
   - Item resolution decoupled from forwarding (path establishment)
2. In-network resources
   - TM nodes → (logically) centralized path/tree formation
3. Stateless multicast forwarding

Compute minimum cost (Steiner) trees for multicast delivery

- Cost of optimization:
  - Signaling cost: resolve the subscription
    - analogous to a DNS or DHT resolution
  - Computation delay at TM

- Evaluation: Emulation of AS 224 (Norwegian Univ. & Research Network)
  - 233 routers, 75 access routers → 75 PSI access networks...
  - For 90% of subscriptions, delay (Steiner - Shortest-path) < 2ms; For 99.6%, < 60ms
  - Steiner-tree byte footprint compared to Shortest-path trees: - 30%, multiple unicasts: - 48%


polyzos@aueb.gr
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

φSAT: The role of Satellites in FI Services

● **Aim:**
  - To investigate the technical feasibility & business viability of the integration of SatCom with terrestrial ICN architectures

● **Results**
  - Methodology to identify application/service scenarios where the capabilities of SatCom and ICN bring highest techno-economic gains
    - Key **SatCom** capabilities: Broadcast/Multicast, Wide Coverage
    - Key **ICN** capabilities: Data aggregation, Multipath Routing, Mobility Support, In-network Caching
  - Candidate scenarios identified
    - Hybrid Broadcast netTV
    - M2M Communications
    - 4G Backhauling
  - Socio-economic evaluation
    - Market evolution for each scenario
Conclusions

- ICN is well positioned to address
  - caching, mobility, multihoming, traffic management/QoS, security...
  - evolution: **tussles resolved at or near run-time**

- PSI chose
  - specific name/ID resolvers (for each scope: RP), rather than flooding
  - separation or functions
    - **separate forwarding** from resolution (no reverse path)
      - centralized aspects, optimizations, policies
      - well matched to SDN/OpenFlow—all optical forwarding

- The PSI architecture inherits the advantages of
  - **ICN** & the **publish/subscribe** paradigm
    - in particular the security ones, but....

- PSI 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): objects, chunks, packets…
- 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?)
- Wireless?

polyzos@aueb.gr
More Observations, Questions & Issues

- Information- vs. Content-centric vs. Named Data vs. pub/sub vs. ...
- overlay vs. clean-slate vs. hybrid/integrated...
  - special-purpose nets only? Not global?
- Rendezvous
  - powerful
  - trusted
    - has lots of information...
  - target of DOS attacks
  - networks of RPs = RN
  - belongs to different entities than network provider?
  - competing RNs
  - RP functionality needed at multiple & different levels
    - Intranet, global... on a wire...
Thank you!

Information-Centric Networking & the Ψ Architecture

George C. Polyzos

Faculty: V.A. Siris, G. Xylomenos, G. Marias
PostDocs: C.N. Ververidis, K.V. Katsaros, P. Frangoudis
Doctoral cand.: N. Fotiou, C. Tsiropoulos, X. Vasilakos, C. Stais, I. Thomas

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

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

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

polyzos@cs.ucsd.edu
Related Publications


more … Related Publications


polyzos@aueb.gr
φSAT Scenario #1: Hybrid broadcast netTV

Key drivers for this scenario identification

- DTH Broadcasting: 1st market for telecom satellites
- Unlimited potential for hybrid access
  - To bring a boost of the link capacity
  - To increase availability of service and QoE
  - To add a return link capability for interactive/added-value services
  - To enlarge service offer (e.g. number of programs for linear / on-demand TV) with several service providers
  - To favor partnerships and competitiveness and to lower costs
- In this context, IP/TV over MPEG-based broadcast brings ease and flexibility for service integration
  - Common standards to any access network
  - E.g. service management, native e2e IP transport…
  - New usages and trends of TV consumption
Scenario #1: Hybrid broadcast netTV

GEO Satcom Network

Transit Networks

Content Provider Network

Fixed Access Network (xDSL, Cable,..)

Media Servers

RVS: RendezVous Servers

SD

HD

3D
φSAT Scenario #2: Smart M2M Transport

Smart Transport M2M use case

Key Challenges

• Mobility support

ICN Specific Advantages

• Information collection and dissemination to/from multiple sources/sinks
• Information aggregation
• Traffic Prioritization
• Mobility support
• Delay tolerant communications
• Reliable real-time SW upgrading
SAT Scenario #3: Extended 4G Backhauling

Key driver for this scenario
- Provides advantages in SatCom integration within the 4G/mobile Internet context given the aggressive video traffic growth levels in terrestrial mobile networks.
- Integrating satellite in a terrestrial 4G infrastructure allows Service Providers to extend their services towards isolated areas and enhance network capabilities for more efficient video content delivery, such as Evolved Multimedia Broadcast Multicast (eMBMS).

Satellite Network Configuration
- GEO or MEO topology
- In some areas terrestrial repeaters (such as in systems based on DVB-SH and NGH) could also be used to boost the satellite signal, e.g. for reception in urban areas (Hybrid satellite –LTE system).

ICN potential
- QoS based inter-component handover management
- Opportunistic/proactive caching for satellite backhauled BS
- Traffic Aggregation & Caching for operator managed VAS
φSAT Scenario #3: Extended 4G Backhauling