Information-Centric Networking Privacy

George C. Polyzos

Mobile Multimedia Laboratory

Department of Informatics
School of Information Sciences and Technology
Athens University of Economics and Business
Athens 113 62, Greece

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

Tel.: +30 210 8203 650, Fax: +30 210 8203 325

PSIRP
PUBLISH-SUBSCRIBE
INTERNET ROUTING
PARADIGM

PURSUIT

φSAT
esa

EIFFEL

AUEB/MMlab **Collaborators**

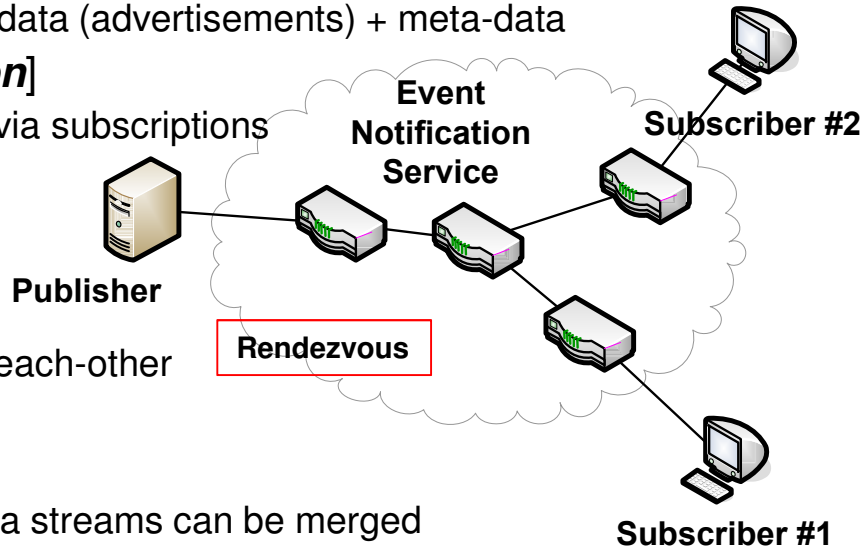
Faculty:	*G. Marias, V.A. Siris, G. Xylomenos*
PostDocs:	*C.N. Ververidis, K.V. Katsaros, P. Frangoudis*
PhD students:	*N. Fotiou, C. Tsilopoulos, X. Vasilakos, C. Stais, I. Thomas*

euronf
NETWORK OF EXCELLENCE

mmlab
Mobile Multimedia Laboratory

Information-Centric Networking (ICN) … in a nutshell

- Information or Content-Centric Networking (**ICN** or CCN) or Named Data…
  - **CCN** is a specific (PARC) project and is a specific architecture and CCNx its implementation
  - Named Data Networking (**NDN**) is an NSF project and architecture, related to CCN
  - Publish Subscribe Internetworking (**PSI**) is an architecture developed by FP7 PSIRP & PURSUIT
- 1st **ACM SIGCOMM ICN** Conference, Paris, France, Sept. 2014.
- **IRTF ICNRG**
- **Publishers** (data 'holders' ← producers/owners) [***publication***]
  - Announce availability of pieces of information/data (advertisements) + meta-data
- **Subscribers** (data consumers) [***subscription***]
  - Express interest in pieces of information/data via subscriptions
- **Rendezvous Network**
  - Matches subscriptions with publications
- Endpoint decoupling (pub-sub)
  - Publishers-Subscribers need not be aware of each-other
  - Asynchronous communication
- Multicast
  - Multiple subscriptions can be grouped and data streams can be merged
- Caching
  - Suitable for in-network on-path and off-path caching



ICN Characteristics & Tradeoffs

ICN vision

- Enabler for FI, IoT, Cloud, 5G…
- Information is key
- Balancing the power between tx-rx
- Better resource utilization
  - **Caching** / pointer operations
  - Network is **data-aware**
    - Name/ID & metadata
- multicast, multi-homing & mobility
- Security addressed @ design time
- Better(?) Privacy

PSI vs. CCN/NDN

- **PSI**: uncoupled Resolution/Routing
- **CCN**: coupled Resolution/Routing
  - better for ad hoc nets / **robust**
    - **flooding** of interests

PSI characteristics

- **SDN similarities**
  - **fast, predetermined forwarding**
  - centralized decisions/flows/paths
- Reliance on ***Rendevous Network***
  - but many RNets, independent
  - strength: prof. mgmt., reputation
  - **trust-to-trust** instead of E2E

Privacy inherent in ICN (?)

- **publishers do not know subscribers:** forwarding techniques that do not reveal destination(s)
  - PSI: zFilters (Bloom filters on links)
  - CCN/NDN: crumb based routing
- pub/sub msgs: sensitive info?
  - **Yes** for PSI, **No** for interests in CCN

Privacy and ICN—The Issues

- The power of the (Rendezvous) Network
  - PSI: explicit requests with requestor ID to Rendezvous Network
  - CCN/NDN: requests to the whole network without requestor ID
    - but implicit ID based on proximity/reverse path
  - Explicit protection from the Rendezvous Network
    - through ***homomorphic encryption***
  - Access Control ***Delegation*** as a privacy enhancing technique
    - … for Access Control policies
- Privacy attacks based on inherent ICN properties
  - e.g., low(er) delay → cached nearby → neighbor requested it…
  - monitoring, decisional interference, and invasion attacks
- A common ICN reference model to study privacy
  - system, adversaries, and threats models
  - evaluating design choices for: **naming, advertisement, resolution, forwarding**

N. Fotiou, S. Arianfar, M. Sarela, G.C. Polyzos, "**A Framework for Privacy Analysis of ICN Architectures**," APF'14.

- Applicability of ICN techniques to the IoT: privacy concerns
- **Challenge**: Protect user privacy & unleash the full potential of ICN

Thank you!

Information-Centric Networking Privacy

George C. Polyzos

Mobile Multimedia Laboratory

Department of Informatics

School of Information Sciences and Technology

Athens University of Economics and Business

Athens, Greece

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

Selected Publications

- G. Xylomenos, C.N. Ververidis, V.A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K.V. Katsaros, G.C. Polyzos, "**A Survey of Information-Centric Networking Research**," ***IEEE Communications Surveys and Tutorials*** (online, 7/2013).
- N. Fotiou, G.F. Marias, G.C. Polyzos, "**Access Control Enforcement Delegation for Information-Centric Networking Architectures**," ACM SIGCOMM ***Computer Communication Review***, 10/2012.
- N. Fotiou, D. Trossen, G.F. Marias, A. Kostopoulos, G.C. Polyzos, "**Enhancing Information Lookup Privacy through Homomorphic Encryption**," ***Security and Communication Networks*** (online 11/2013).