ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Information-Centric Networks

Section # 9.3: Clean Slate

Instructor: George Xylomenos

Department: Informatics

European Union
European Social Fund

OPERATIONAL PROGRAMME
EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION, LIFELONG LEARNING AND RELIGIOUS AFFAIRS
MANAGING AUTHORITY

NSRF 2007-2013
programme for development
EUROPEAN SOCIAL FUND

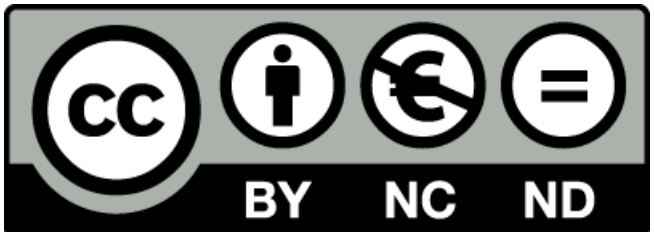
Co- financed by Greece and the European Union

Funding

- These educational materials have been developed as part of the instructors educational tasks.
- The **“Athens University of Economics and Business Open Courses”** project only funded the reformatting of these educational materials.
- The project is being implemented as part of the Operational Program “Instruction and Lifelong Learning” and is co-financed by the European Union (European Social Fund) and national funds.

Licencing

- These educational materials are subject to a Creative Commons License.



Week 9 / Paper 3

- VoCCN: Voice Over Content-Centric Networks
  - V. Jacobson, D. K. Smetters, N. H. Briggs, M. F. Plass, P. Stewart, J. D. Thornton, R. L. Braynard
  - ACM ReArch 2009
- Main point
  - Content-centric targets fetching/downloading applications
  - Can it work for other applications, too?
    - E-mail, streaming and (especially) VoIP?
  - VoCCN: Voice over CCN (instead of IP)
  - Based on certain key properties of CCN

Introduction

- Most new architectures place content at the center
  - Good fit for content exchange applications (WWW, P2P)
  - What about conversational applications (VoIP, e-commerce)?
- VoCCN addresses the issue of CCN suitability
  - Real-time, conversational, telephony over CCN
  - Simpler, more secure and more scalable than VoIP
  - Uses SIP and RTP to securely interoperate with VoIP
  - Employs a stateless IP to CCN gateway
  - Model for mapping conversational applications to CCN

VoIP background

- VoIP components
  - Endpoints are represented by fixed proxies
    - The endpoints can be mobile or have dynamic IP addresses
  - Signaling established via SIP (Session Initiation Protocol)
    - Caller to caller's proxy, to callee's proxy, to callee
    - The proxies must know where the endpoints reside
  - Data exchange directly between endpoints
    - The caller's invite indicates its address for RTP data
    - The callee's accept indicates address for RTP data
  - Media can be secured via SRTP or tunneling inside DTLS
  - Signaling can be secured via DTLS/PKI or MIKEY
    - Authentication and encryption are tricky to setup
    - Usually everything ends up unencrypted and unathenticated!

Architecture

- VoIP is harder than it needs to be
  - The caller simply wants to talk to the callee
  - The network requires finding the callee's phone IP address
    - This is where the SIP proxies come into play
  - In content-oriented networking this should be redundant
- VoCCN has to solve a different set of problems
  - Service rendezvous: the callee must offer a contact point
    - In IP this is the TCP/UDP port to which the application listens
  - In CCN we must request content that has not been published
    - The network must route the request to potential publishers
    - The publishers should then create and publish the content

Architecture

- VoCCN has to solve a different set of problems
  - The service rendezvous must transition to a conversation
    - In IP the SIP packets contain information in an SDP payload
  - In CCN we need dynamically constructible names
    - Construct the name of a piece of content without being told
- Two requirements for content name construction
  - Deterministic algorithm to produce names
    - Names rely on information available to both endpoints
    - Cannot use (say) content hashes as names
  - Support for partial specification of names
    - Constructing unique names requires prearrangement
    - Partial names allow unique names to be used eventually
  - Structured names can satisfy both requirements

Architecture

- In CCN content uses hierarchical naming
  - Interest packets specify a name prefix and some rules
    - The rules specify what matching content to return
  - CCN routers use prefix matching to direct Interests
    - Sent towards content sources that have registered availability
  - Sources do not need to register the exact content, only prefixes
    - Content can be generated on the fly
  - Data packets reverse the path taken by interests
- VoCCN signaling
  - Each VoCCN endpoint has an identity (e.g. alice@ccnx.org)
  - The endpoint registers to offer data in a specific namespace
    - Based on service and identity (e.g. /ccnx.org/sip/alice/invite)

Architecture

- VoCCN signaling
  - A caller sends an Interest asking for content from the callee
    - The well-known prefix is extended with unique data
    - A session key encrypted with the callee's public key
    - The SIP invite data encrypted with the session key
  - The callee responds with a data packet generated on the fly
    - Uses the name indicated by the caller
    - Includes the SIP accept data encrypted with the session key
- VoCCN data exchange
  - Uses a sequence of names based on rendezvous information
    - Call-id+endpoint+sequence (e.g. /ccnx.org/alice/call-id/rtp/seqno)
    - Each Interest is matched by a unique data packet
  - Can issue many interests to pipeline data flow
    - As data packets arrive, more interests are generated

Advantages

- Easy location of endpoints
  - In IP the endpoint needs to register its IP address with a proxy
  - With CCN a prefix can be registered at many areas
    - The Interest will be routed to all of them
    - The endpoint will respond from its current location
- Endpoints can prove their identity
  - All the credentials needed are at the endpoint
    - The private key needed to decrypt the session key
  - No need to change identity to IP address mappings
- Advanced services are easy to build
  - Exploits the built-in multipoint routing of CCN
    - Follow call requests or copy and process call contents

VoCCN/VoIP interoperability

- Based on a stateless VoCCN/VoIP gateway
  - SIP and SRTP are used to simplify the exchange
  - The gateway acts as a SIP proxy that translates packets
  - A SIP/SRTP packet is translated to a CCN data packet
    - They match CCN interest packets from VoCCN endpoints
    - The gateway also generates an Interest for the next packet
    - This matches the next data packet from the VoCCN endpoint
    - The VoCCN packet is translated to an IP packet
  - The proxy does not maintain state on conversations
    - Every action is based on received packets
  - Signaling security is provided for the CCN part only
    - The IP part may have its own SIP signaling security mechanism
    - End-to-end data security does not involve the gateway

Implementation

- Implementation data
  - VoCCN client based on Linphone
    - Uses extensible SIP and RTP libraries
    - Simple plugins for the CCN part
  - CCN routers on all routers and endpoints
    - CCN routers communicate over a UDP overlay
- Security
  - Many ways to get public keys in CCN
    - Ask for /ccnx.org/users/alice/KEY and accept on faith
    - Publish key as CCN content signed by a trusted third party
  - VoCCN used MIKEY to secure the data exchange
    - MIKEY is initiated during the SIP signaling exchange
  - The signaling exchange is protected with public keys

Implementation

- Performance
  - Direct exchange between two machines in the same LAN
  - Compared stock Linphone with VoCCN version
  - No perceptible impact from packet signing with 1024 bit RSA keys
  - No packet loss, but some delayed packets in the latter case
  - Similar jitter for both versions

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

End of Section # 9.3

Course: Information-Centric Networks, **Section # 9.3: Clean Slate**

Instructor: George Xylomenos, **Department:** Informatics

European Union
European Social Fund
OPERATIONAL PROGRAMME EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION, LIFELONG LEARNING AND RELIGIOUS AFFAIRS
MANAGING AUTHORITY
NSRF 2007-2013
programme for development
EUROPEAN SOCIAL FUND
Co- financed by Greece and the European Union