Empowered by Innovation NEC

Ongoing Research Activities in the GreenICN Project on "Using ICN in Disaster Scenarios"

Related Drafts:
draft-seedorf-icn-disaster-03
draft-seedorf-icn-wot-selfcertifying-01
draft-jiachen-icn-pubsub-01

Jan Seedorf, Dirk Kutscher, Atsushi Tagami, Kohei Sugiyama, Mayutan Arumaithurai, Yuki Koizumi, Nicola Blefari Melazzi, Tohru Asami, K.K. Ramakrishnan, Tomohiko Yagyu

Contact: Jan.seedorf@neclab.eu

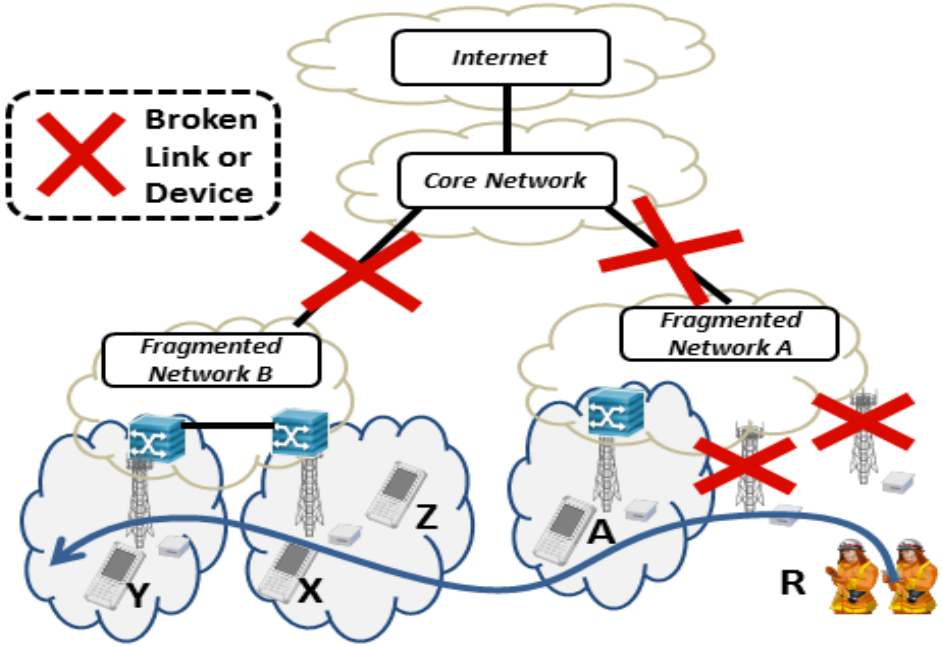
IETF-92, March 2015, *Dallas, Texas, USA*

PROBLEM SPACE & RESEARCH CHALLENGES

Scenario and Use Cases

Disaster Scenario

- The aftermath of a disaster, e.g. hurricane, earthquake, tsunami, or a human-generated network breakdown
- E.g. the enormous earthquake which hit Northeastern Japan on March 11, 2011 (causing extensive damages including blackouts, fires, tsunamis and a nuclear crisis)



Key Use Cases (High-Level)

- Authorities would like to inform the citizens of possible shelters, food, or even of impending danger
- Relatives would like to communicate with each other and be informed about their wellbeing
- Affected citizens would like to make enquiries of food distribution centres, shelters or report trapped, missing people to the authorities

Research Gap

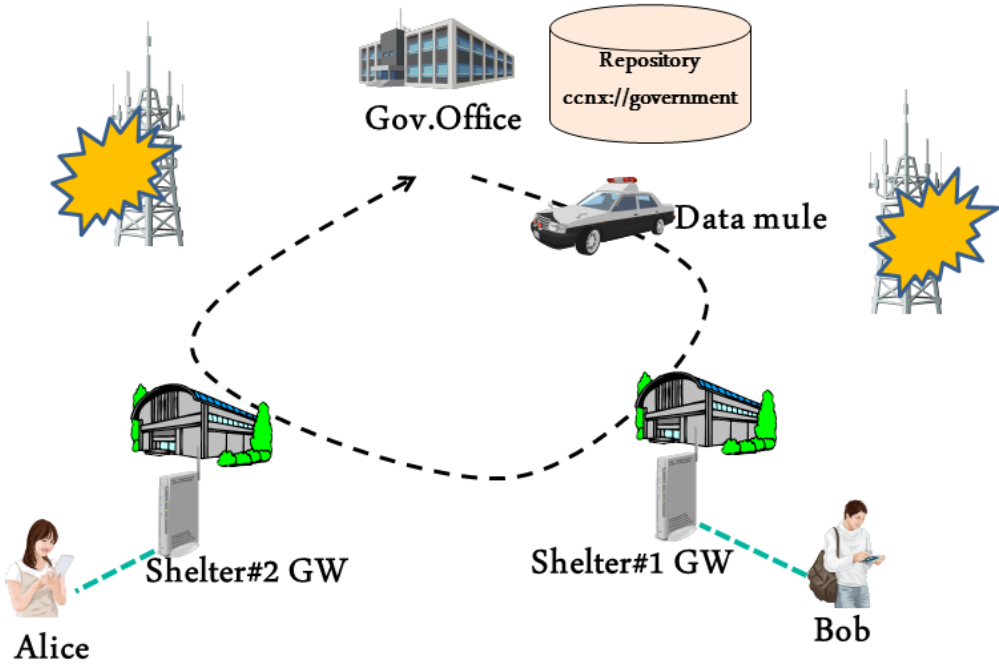
- Quite some work in the DTN community, however most DTN work lacks key features which are needed in the disaster scenarios we consider, such as
  - publish/subscribe (pub/sub) capabilities, caching, multicast delivery, message prioritisation based on content types, …
- Could enhance existing DTN approaches with these features – we argue that ICN makes a better starting point for building a communication architecture that works well before & after a disaster
  - ICN data mules have built-in caches and can thus return content for interests straight on
  - Requests do not necessarily need to be routed to a source (as with existing DTN protocols), instead any data mule or end-user can in principle respond to an interest
  - Built-in multi-cast delivery implies energy-efficient large-scale spreading of important information which is crucial in disaster scenarios
  - Pub/sub extensions for popular ICN implementations exist
  - DTN routing algorithms have been solely designed for particular DTN scenarios; extending ICN approaches for DTN-like scenarios ensures that our solution works in regular (i.e. well-connected) settings just as well (important in reality, where a routing algorithm should work before and after a disaster)

→ Our rationale: start with existing ICN approaches and extend them with the necessary features needed in disaster scenarios

ONGOING RESEARCH AND INITIAL RESULTS

ICN ’Data Mules’

- Mobile entities can act as ICN ’data mules’
  - equipped with storage space, moving around the disaster-stricken area gathering information to be disseminated
  - ICN’s concept of decoupling sender and receiver is very suitable for these ’data mules’
- Approach: Dynamic Name-Based Routing (DSDVN)*
  - A name-based routing protocol for fragmented networks based on the well-known Ad-Hoc routing protocol DSDV
  - Extends DSDV to convey name prefix information in the routing message
  - State of links is set to the Face in CCNx and utilized to control retransmission



ICN Data Mules in a Disaster Scenario

*T. Yagyu and S. Maeda, “Demo Overview: Reliable Contents Retrieval in Fragmented ICNs for Disaster Scenario,” in Proc. of 1st ACM Conference on Information-Centric Networking, ser. ICN, Sep. 2014.

Priority dependent Name-based Replication[1]

Approach: NREP (Name-based Replication)

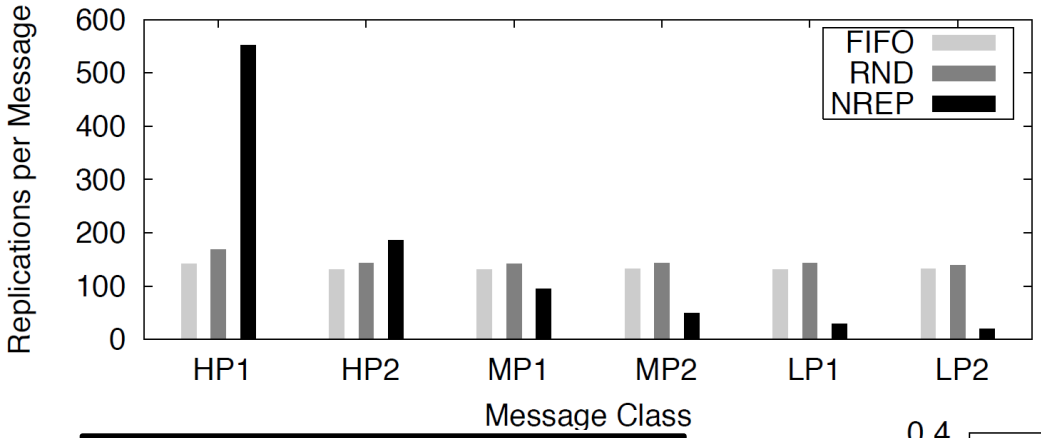
- associate each message generated in a disaster scenario with a *Name + Attributes*
- exploit the information that can be exposed in a content name: *Name-Based Replication*
  - Nodes store-carry-and-forward messages:
    - with specific time and space limits, and
    - with priorities as to what to replicate
  - Time-space limits, as well as priorities are included within the message's name (or attributes field)
- *routing/forwarding decisions are made based on the name*

NREP Design

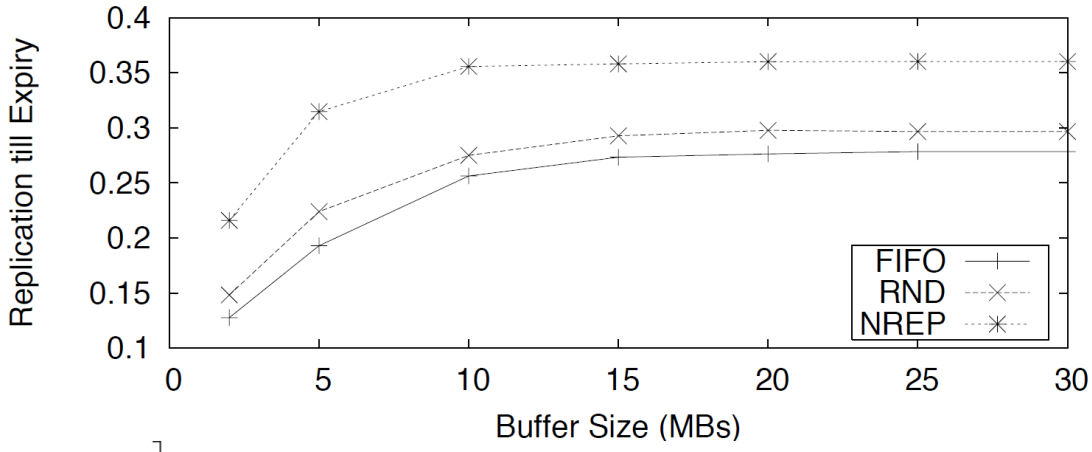
1. *Hierarchical* is working better than flat in this case
   - `Emergency/SOS` or `Warning/Shelter`
   - content can be filtered according to a longest prefix match
   - Namespace has a globally understood prioritisation value
2. The *name* shows the priority
   - `Emergency, Warning, chat`
3. Time and space limits are kept as *attributes*,
   - `boroughX/ttl=2h, radius=Xkm/ttl=Yhours`
4. User-defined priorities kept as attributes too
   - user-perceived importance, e.g., from 1-5 how useful/important was the message

1 - I. Psaras et al., "Name-based replication priorities in disaster cases," in 2nd Workshop on Name Oriented Mobility NOM), 2014.

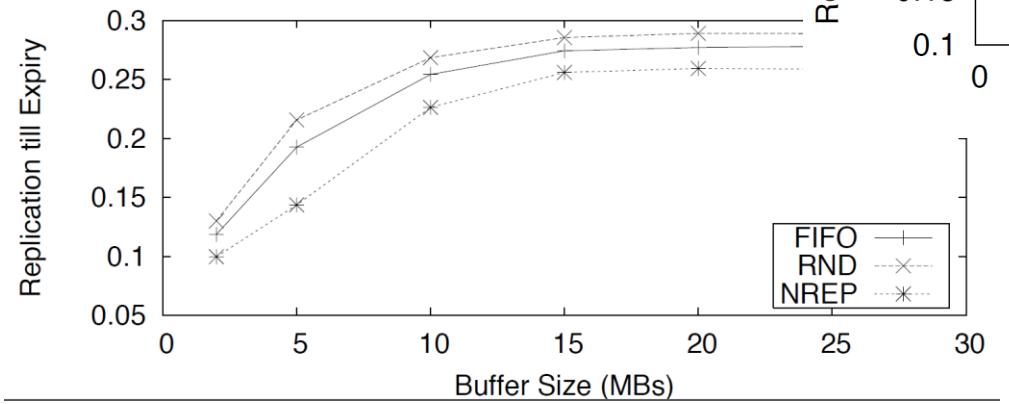
Priority dependent Name-based Replication: Results



Replications Per Message



High Priority Class



Low Priority Class

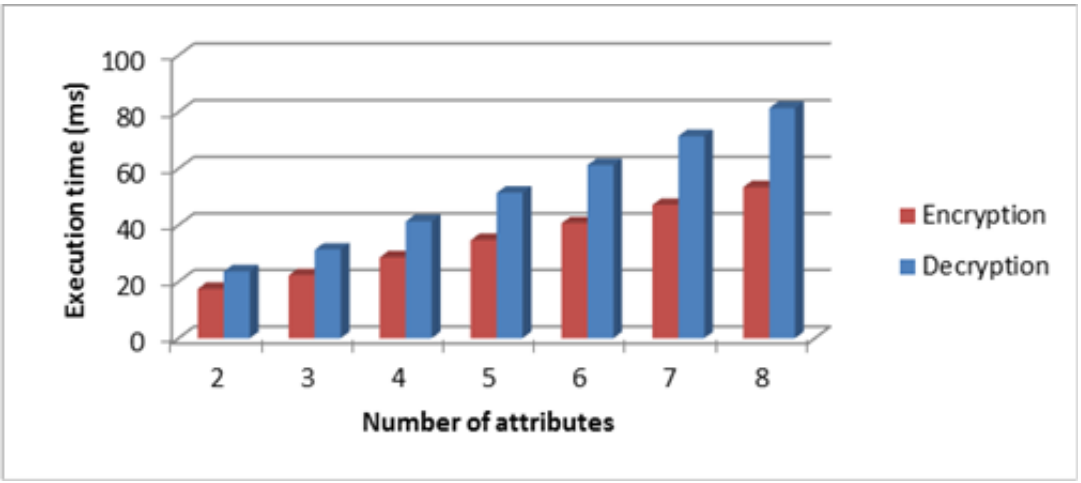
Data-centric Confidentiality and Access Control

- Approach: Use of ’Ciphertext-Policy Attribute Based Encryption’ (CP-ABE)
  - allowing a party to encrypt a content specifying a policy, which consists in a Boolean expression over attributes, that must be satisfied by those who want to decrypt such content
  - Example Policy: allow access only to recipients who fulfill

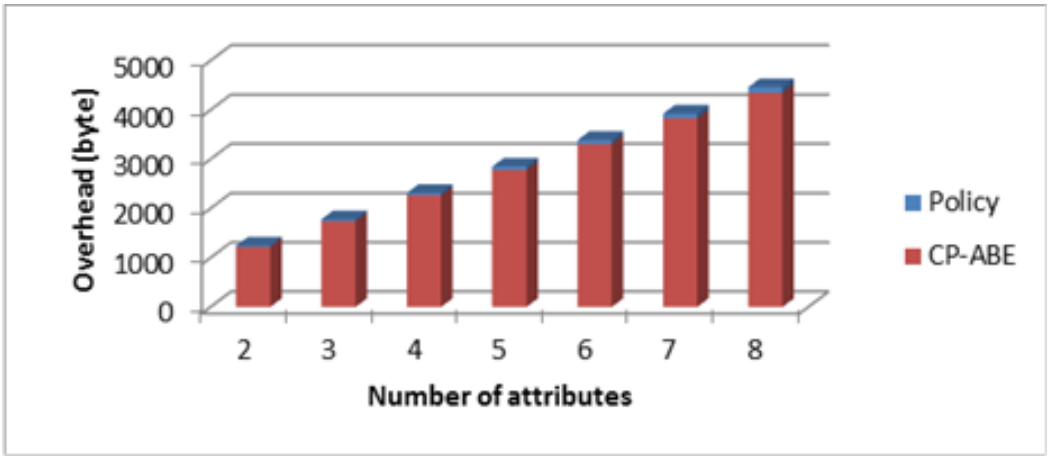
$$\Pi = (\text{job:official} \wedge \text{rank:executive}) \vee (\text{job:emergency} \wedge \text{rank:any})$$

- Our Work / Results*
  - proposed a multi-authority CP-ABE-based security architecture for ICN
  - carried out a performance evaluation, showing that for normal policies (say comprising 2 - 6 attributes) even a Java implementation on a low-end PC requires less than 40ms for encryption (60ms, respectively, for decryption)

Data-centric Confidentiality and Access Control: Results



Execution Time for CP-ABE Encryption and Decryption functions vs number of attributes that form the policy



Overhead introduced in the packet to support the CP-ABE functionalities vs. number of attributes that form the policy

Decentralised Authentication of Messages[1,2,3]

Based on a Web-of-Trust (WoT)

- A so-called *'WoT file'* is being used by terminals
  - can be retrieved from a WoT keyserver before the disaster takes place
  - contains the veried certicate graph for the whole WoT in a compressed, machine-readable format. Terminals thus
- ➢ Terminals have the complete trust relationships within the WoT at their disposal
  - in the from of a 'WoT-graph' stored in a file

Binding between self-certifying ICN names and a Web-of-Trust

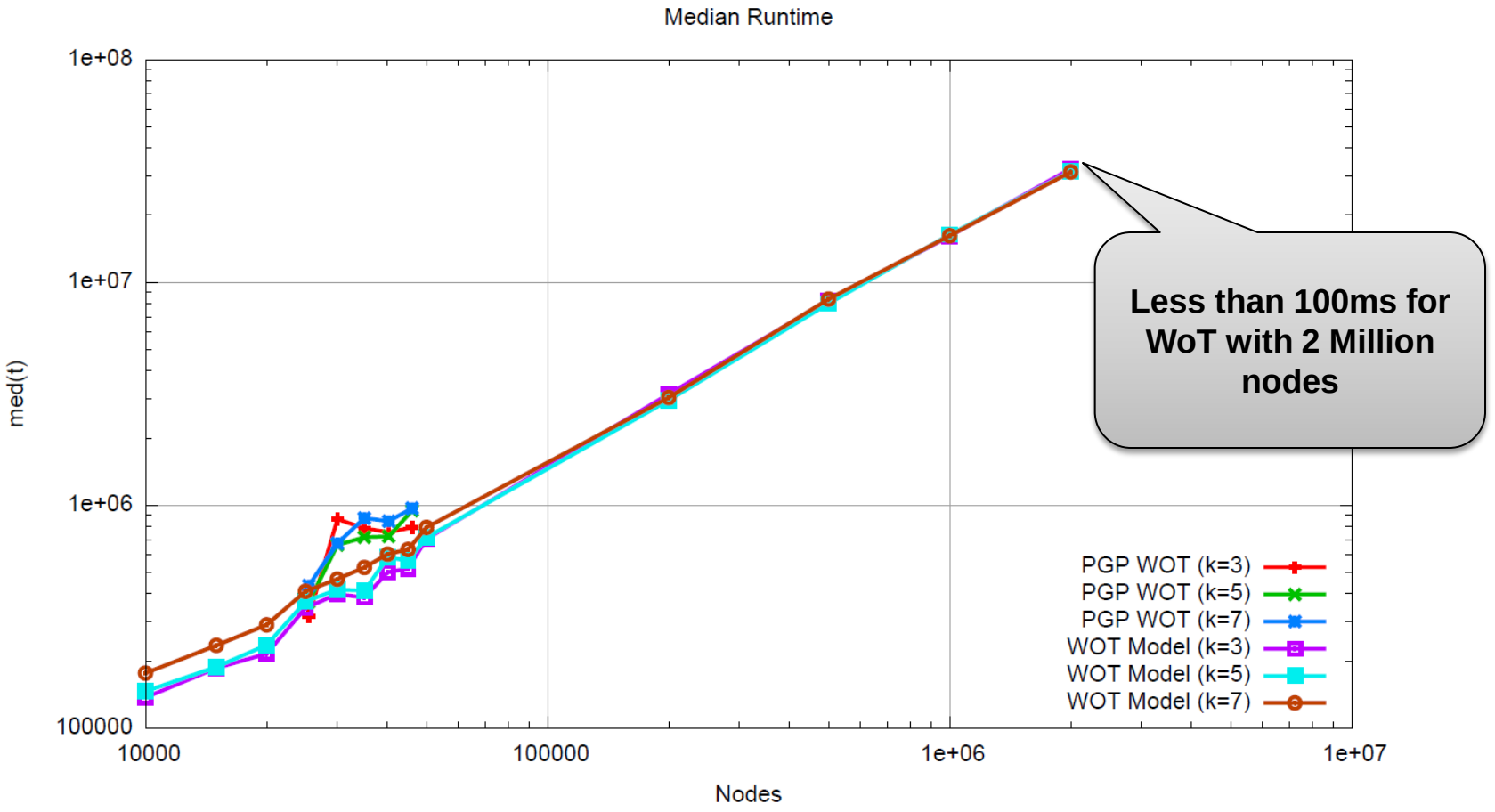
- The WoT key-ID is equivalent to the self-certifying name part used in the ICN naming scheme
- This ties the self-certifying name with the ID of the correct public key in the WoT, and thus transitively with the RWI in the WoT (e.g. email address)

Assessing information received (as a response to a given request for a certain name)

- A double-sided Breadth First Search (`dBFS`) algorithm is executed on the WoT-graph to find certificate chains between the initiator of the request and the publisher of the content
- Depending on a trust metric (see demo for examples) the information received is regarded as trustworthy or not by the initiator of the request
  - trust metric is applied on the result of the `dBFS` algorithm

1 - J. Seedorf, D. Kutscher, and F. Schneider: „Decentralised binding of self-certifying names to real-world identities for assessment of third-party messages in fragmented mobile networks," 2nd Workshop on Name Oriented Mobility (NOM), 2014
2 - J. Seedorf et al.: "Demo overview: Fully decentralised authentication scheme for icn in disaster scenarios (demonstration on mobile terminals)," in 1st ACM Conference on Information-Centric Networking (ICN-2014), 2014.
3 - J. Seedorf: „draft-seedorf-icn-wot-selfcertifying-01"

Decentralised Authentication of Messages: Results



Runtime (in ns) for Decentralised Authentication Approach on Web-of-Trust Graphs of various Sizes (Median)

Energy Efficiency

Considering 3 approaches

- Priority control
  - name-based prioritisation on routing/forwarding
- cell-zooming
  - switching-off some of the Base Stations because switching-off is the only way to reduce power consumed at idle time
- collaborative upload
  - end-devices delegate sending/receiving messages to/from a base station to a representative end-device with radio propagation of better quality
  - complementary to cell zooming

Ongoing Work

- Started with the design of an ICN-based publish/subscribe protocol that incorporates collaborative upload*

* See also: M. Arumaithurai et al.: „draft-jiachen-icn-pubsub-01“

Acknowledgements

Acknowledgement: This work has been partially supported by the GreenICN project (GreenICN: Architecture and Applications of Green Information Centric Networking), a research project supported jointly by the European Commission under its 7th Framework Program (contract no. 608518) and the National Institute of Information and Communications Technology (NICT) in Japan (contract no. 167). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the GreenICN project, the European Commission, or NICT.

Background: GreenICN Project

- **GreenICN: Architecture and Applications of Green Information Centric Networking**
- Duration: 3 years (1 Apr 2013 – 31 Mar 2016)
- Website: http://www.greenicn.org

EU Coordinator:	JP Coordinator:
Prof. Xiaoming Fu	Mr. Shigehiro Ano
University of Göttingen	KDDI R&D Labs
Germany	Japan

Project Consortium

European Partners

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

EU Coordinator

Georg-August-Universität Göttingen (UGO, Germany)
Contact: Xiaoming Fu <fu@cs.uni-goettingen.de>

NEC Europe Ltd. (NEE, UK)

CEDEO (CED, Italy)

Telekomunikacja Polska (Orange Labs, Poland)

University College London (UCL, UK)

Japanese Partners

KDDI R&D LABS

JP Coordinator

KDDI R&D Laboratories Inc. (KDD, Saitama)
Contact: Shigehiro Ano <ano@kddilabs.jp>

NEC Corporation (NEJ, Tokyo)

Panasonic Advanced Technology Development Co., Ltd

University of Tokyo (UTO, Tokyo)

Waseda University (UWA, Tokyo)