Using ICN in disaster scenarios
(draft-seedorf-icn-disaster-00)

M. Arumaithurai, **J. Seedorf** , A. Tagami, K. Ramakrishnan, N. Blefari Melazzi

IETF 87, Berlin
ICNRG
August 2013

Outline

1. Background of this Work
   – GreenICN Project Overview

2. Using ICN in disaster scenarios
   – What disasters are we talking about
   – Research challenges
   – Why ICN approaches may be promising

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

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

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)

GreenICN Objectives

- ICN: A new networking paradigm where the network provides users with named content, instead of communication channels between hosts
  - **Many issues stay open:** naming, routing, resource control, security, privacy and migration path from today's Internet
  - **Missing seamless support of content-based publish/subscribe** for efficient information dissemination
  - Existing solutions do **not** sufficiently **address energy efficiency**

- GreenICN 's scientific aim:
  - Develop innovative methodologies and approaches to optimize ICN paradigm in a highly-scalable and energy-efficient manner
  - Support two use scenarios: **disaster recovery**; **video delivery**

Focus of **draft-seedorf-icn-disaster-00**

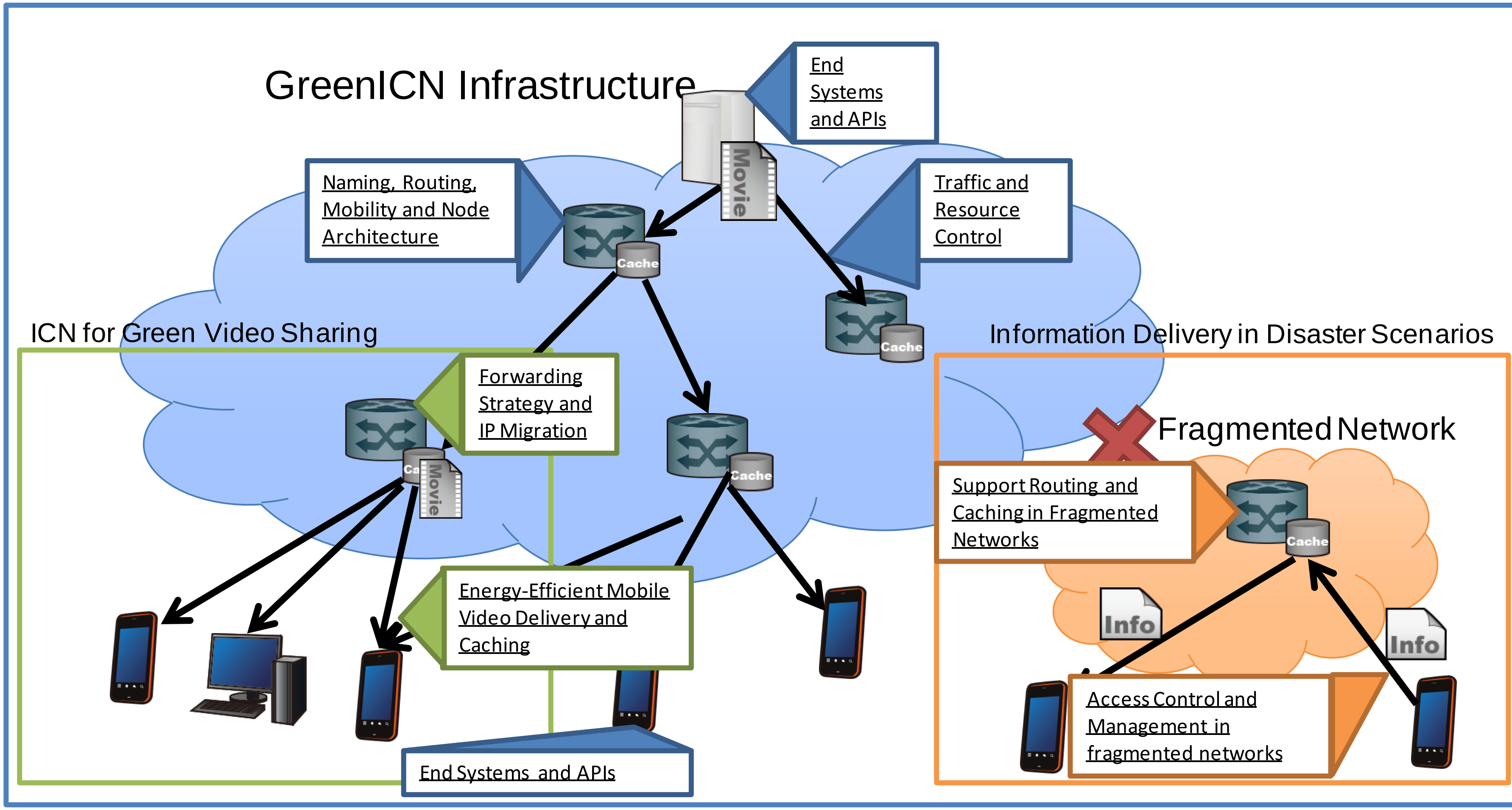
Goals

- Requirement 1: 20% Reduction of Power Consumption of GreenICN for Normal Days
  - EU announced that the total energy consumption of all EU countries should be decreased by 20%.
  - Japan announced a reduction of energy consumption of 30% by 2030, compared to that in 2003.
- Requirement 2: At Least 40% Reduction of Power Consumption of GreenICN (including end-user devices) for Disasters
  - In 2011, people in Tohoku area suffered 3 days of blackout because of the East Japan Earthquake.
  - The 40% reduction aims to make the communication services and related base stations able to operate 3 days in such a scenario.

Goals (Continued)

- Requirement 3: Seamless Services before and after a Disaster
  - The lesson learned at the 2011 East Japan Earthquake is that terminals and services specifically designed for disasters were useless, and that people wanted to use the same terminals and services used in their everyday life.
- Requirement 4: Migration Path
  - GreenICN should friendly coexist with the current IP network
- Requirement 5: Scalability and size of the served contents and related names
  - GreenICN should be able to serve at least current Web contents with off-the-shelf technology

GreenICN Architecture

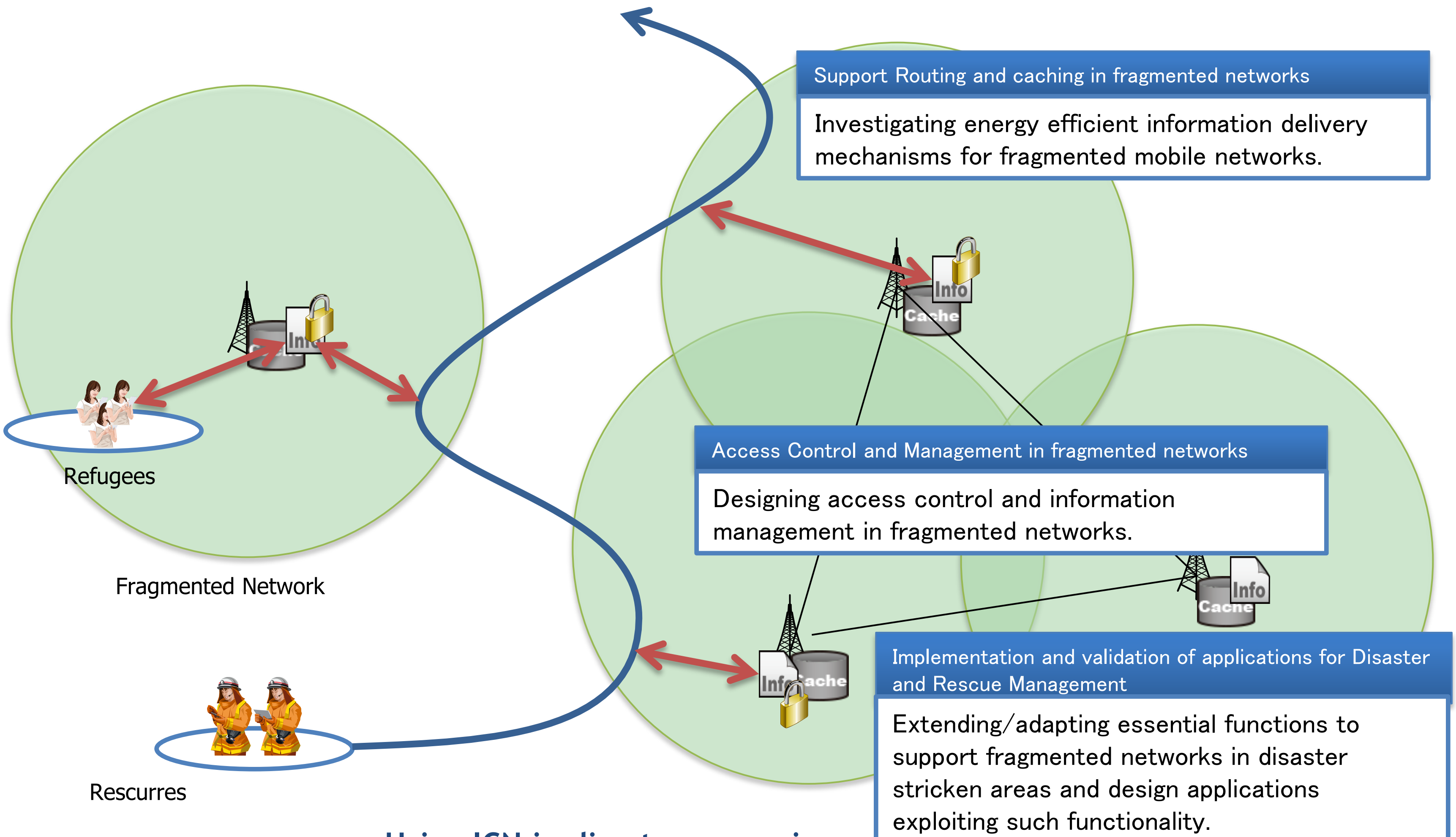


Disaster Scenarios

- **What scenarios are we considering?**
  - 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 (Tohoku areas) on March 11, 2011, and caused extensive damages including blackouts, fires, tsunamis and a nuclear crisis
- **What are the constraints and requirements in such situations?**
  - Energy and communication resources are at a premium
    - E.g. due to failure of certain devices and communication links
  - It is critical to efficiently distribute disaster notification and critical rescue information
    - 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

Vision: Green Disaster Information Delivery and Rescue Management

- Objective: Provide support for large-scale energy-efficient disaster information delivery for fragmented/disrupted mobile networks, including routing and cache management algorithm for highly fragmented networks



Using ICN in disaster scenarios

High-Level Research Challenges

- Enabling usage of functional parts of the infrastructure, even when these are disconnected from the rest of the network
  - it is desirable to be able to continue using functional components for communication as much as possible
  - challenging when these components are disconnected from the backhaul, thus forming fragmented networks
- Decentralised authentication
  - In today's mobile networks, users are authenticated via central entities; in order to communicate in fragmented or disconnected parts of a mobile network, the challenge of decentralising user authentication arises
  - data origin authentication of content retrieved from the network is challenging when being 'offline' (e.g. disconnected from servers of a security infrastructure such as a PKI)
- Delivering/obtaining information in congested networks
  - Significant congestion can be expected in parts of the infrastructure due to broken cables, failed routers, etc.
  - even more important as in the case of a disaster aftermath, it may be crucial to deliver certain information to recipients (e.g. warnings to citizens)

How ICN can be Beneficial

- Routing-by-name
  - very handy in a fragmented network where reference to location-based, fixed addresses may not work as a consequence of disruptions
  - for instance, name resolution with ICN does not necessarily rely on the reachability of application-layer servers (e.g. DNS resolvers)
- Authentication of named data objects
  - With 'self-certifying data' approaches, the origin of data retrieved from the network can be authenticated without relying on a trusted third party or PKI
- Content-based access control
  - ICN can regulate access to data objects (e.g. only to a specific user or class of users) by means of content-based security
  - this functionality could facilitate trusted communications among peer users in isolated areas of the network
- Caching
  - Caching helps in handling huge amounts of traffic, and can help to avoid congestion in the network (e.g. congestion in backhaul links can be avoided by delivering content from caches at access nodes)

Acknowledgements

This work has been 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.