On the intersection of Information Centric Networking and Delay Tolerant Networking (Lessons learned from the GreenICN project)

Hochschule
für Technik
Stuttgart

Jan Seedorf
HFT Stuttgart

Visit at HAW Hamburg
December 2019

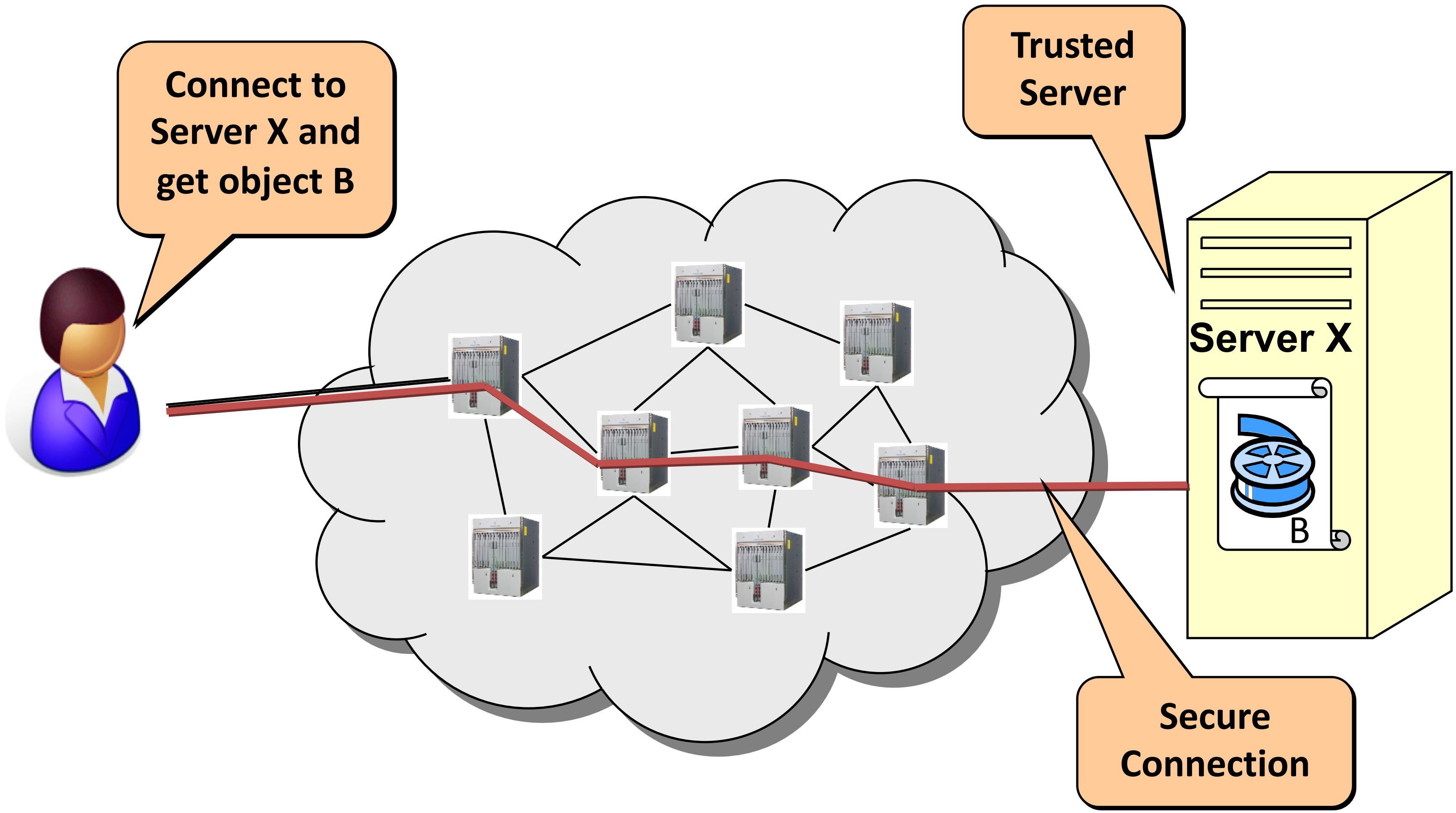
Outline

- (Very) Short Introduction to Information Centric Networking
- GreenICN Project Background
  - Disaster Scenario
  - Rationale
- Overview on selected Solutions
  - …which we developed and evaluated
- Deep Dive
  - Decentralised ICN Interest Popularity Estimation
- Lessons Learned & Open Questions
  - Key Takeaways
  - Remaining Issues & Challenges
  - Discussion

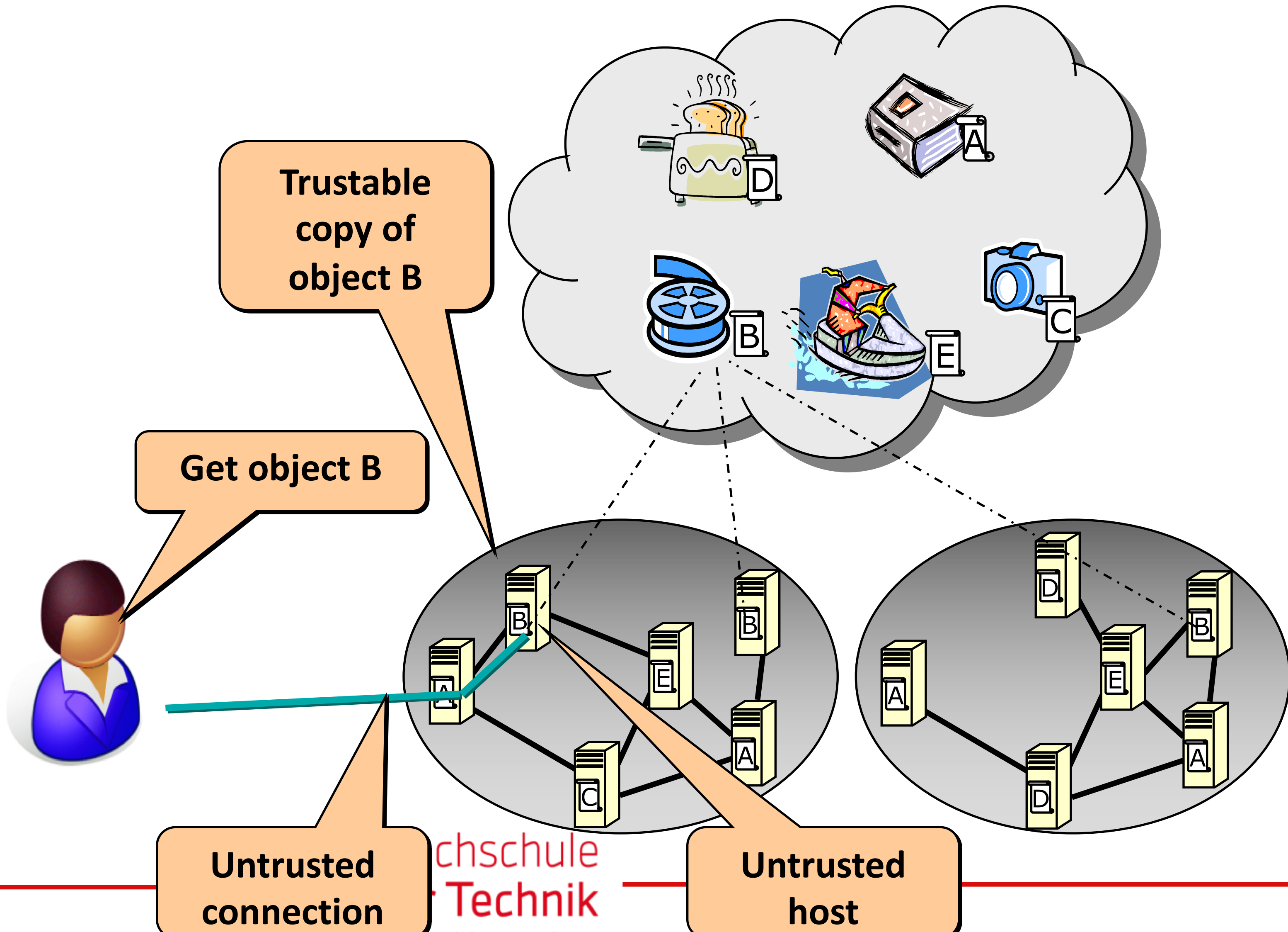
Hochschule
für Technik
Stuttgart

(Very) Short Introduction to Information Centric Networking

Host-centric networking



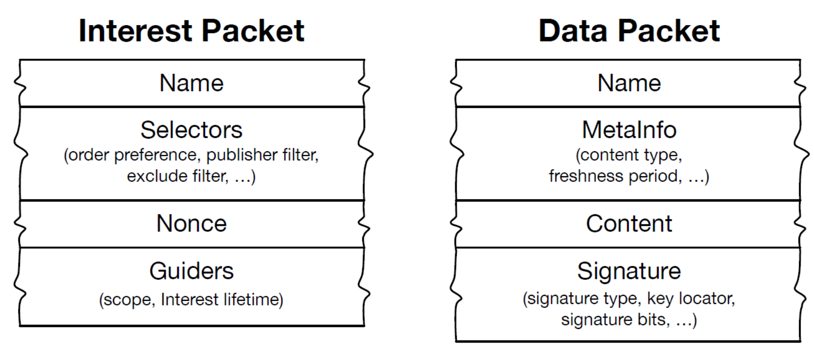
Information-Centric Networking



Credits: Prof. Dr. Dirk Kutscher (Hochschule Emden/Leer)

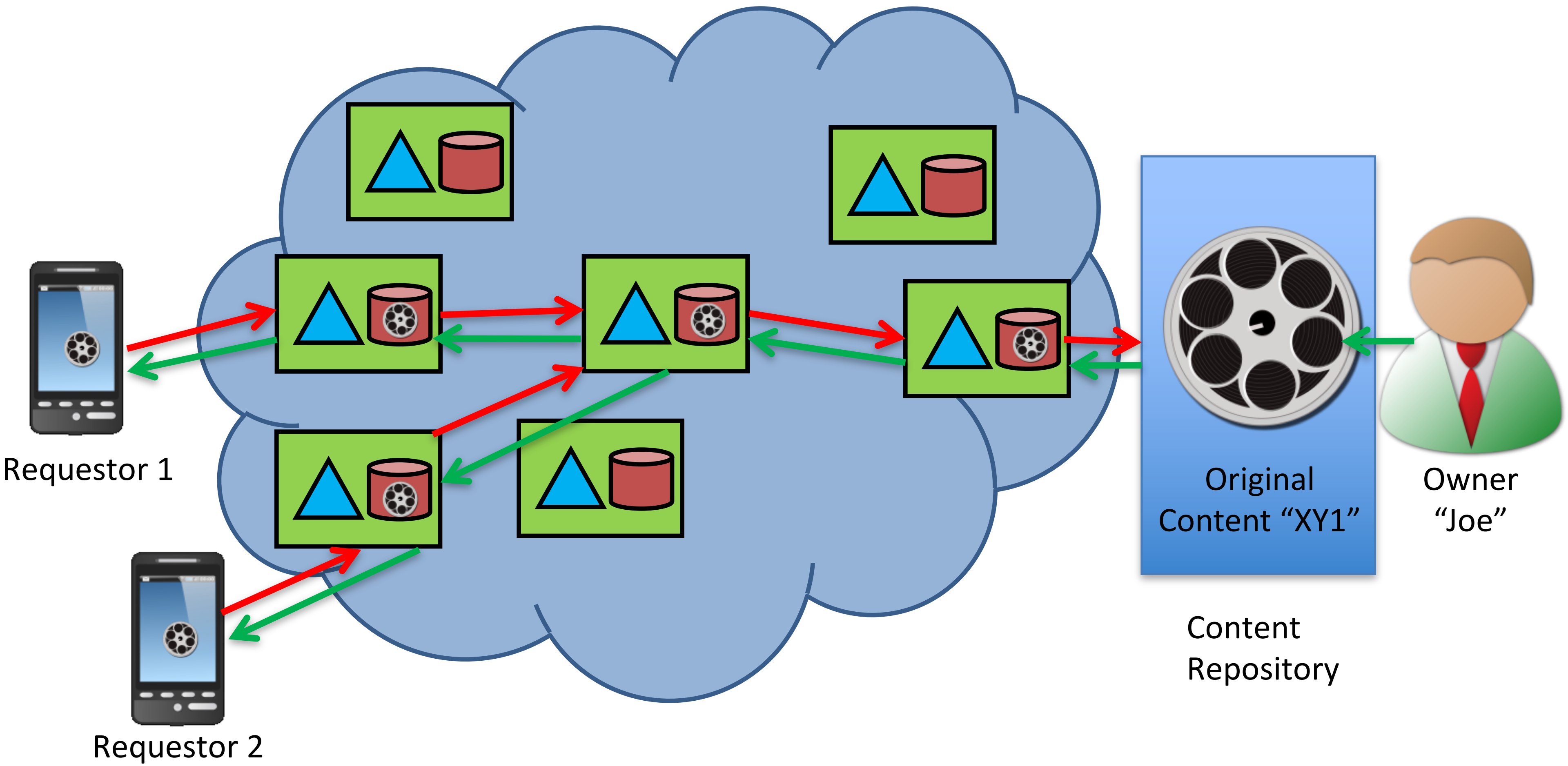
ICN communication model

- Clients (C) send **requests (Interest Packets)** asking for named data
- Routers (R) in the network route requests towards publishers (P)
- Any node with a cached copy can provide the corresponding **information object (Data Packet)**
- Pending Interest Table (PIT): ”stores all the Interests that a router has forwarded but not satisfied yet“ [https://en.wikipedia.org/wiki/Named_data_networking]
- *Remark:*
  - On the surface, this is exactly the service of HTTP, but the request is there always addressed to a particular host



*ICN Packet examples**

ICN-based Information Retrieval 101



Credits: Prof. Dr. Dirk Kutscher (Hochschule Emden/Leer)

ICN Core Properties

- **Accessing named data as a first-order network principle**
  - Transmission of self-contained units
- **Name-content-binding validation and other security services based on object/naming security**
  - Not based on connection security
- **Ability to leverage ubiquitous in-network memory**
  - Rate adaptation
  - Repair (efficient re-transmissions)
  - Sharing (Re-use)

Hochschule für Technik Stuttgart

GreenICN Project Background

Background: GreenICN Project

- **GreenICN: Architecture and Applications of Green Information Centric Networking**
- Duration: 3,16 years (1 Apr 2013 – 31 May 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

SEVENTH FRAMEWORK PROGRAMME

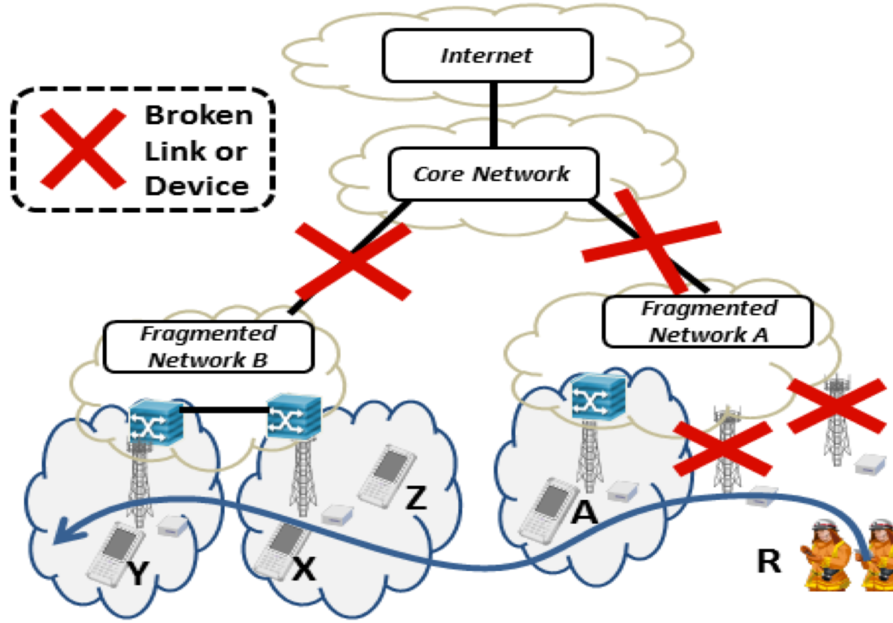
NICT

Hochschule für Technik Stuttgart

Project Consortium

European Partners	Japanese Partners
EU Coordinator Georg-August-Universität Göttingen (UGO, Germany) **Contact:** Xiaoming Fu <fu@cs.uni-goettingen.de>	**JP Coordinator** KDDI R&D Laboratories Inc. (KDD, Saitama) **Contact:** Shigehiro Ano <ano@kddilabs.jp>
NEC Europe Ltd. (NEE, UK)	NEC Corporation (NEJ, Tokyo)
CEDEO (CED, Italy)	Panasonic Advanced Technology Development Co., Ltd
Telekomunikacja Polska (Orange Labs, Poland)	University of Tokyo (UTO, Tokyo)
University College London (UCL, UK)	Waseda University (UWA, Tokyo)

Scenario and Use Cases



Disaster Scenario

- The aftermath of a disaster
  (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 incl. blackouts, fires, tsunamis and a nuclear crisis)

➢ **Energy and communication resources are at a premium**

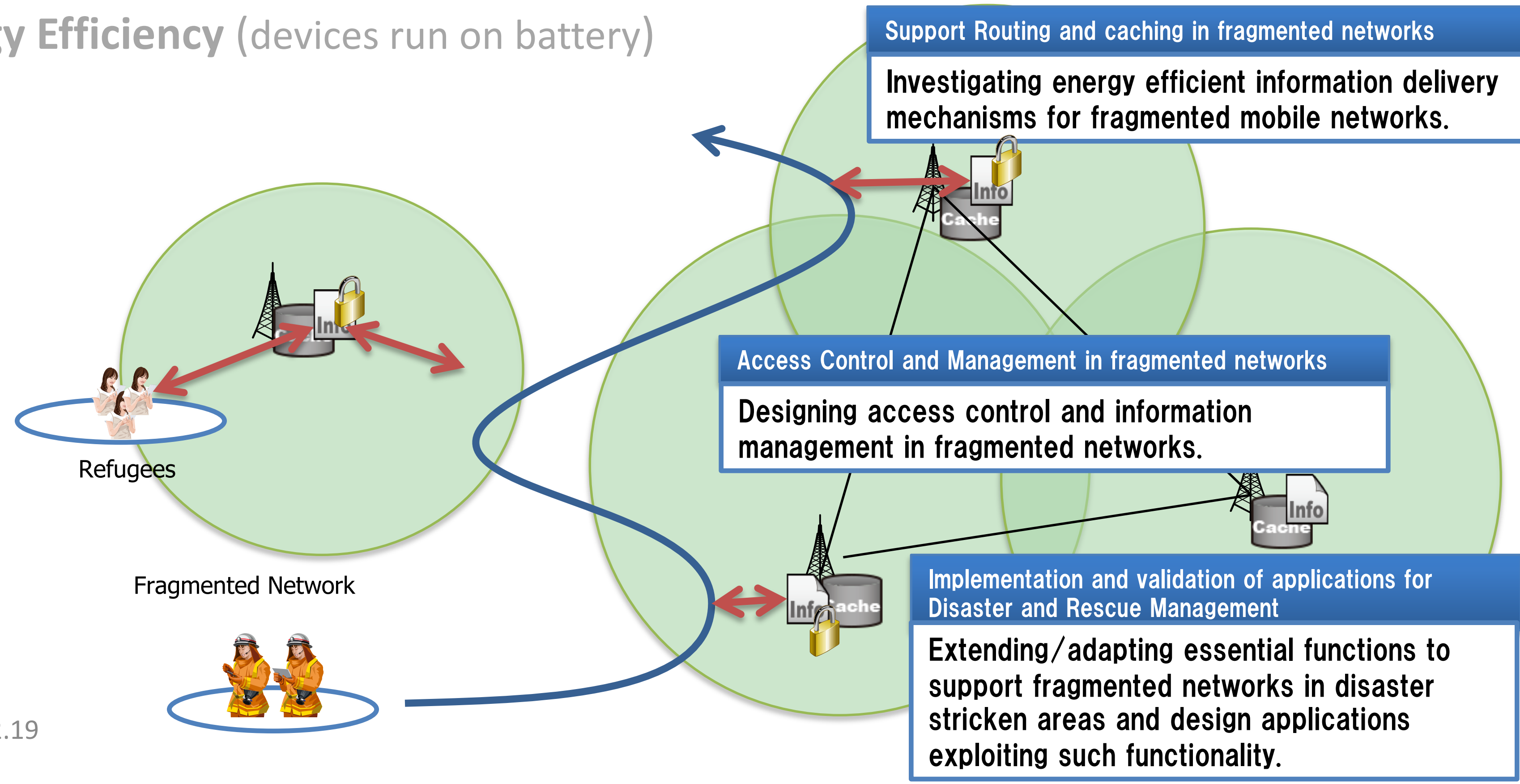
➢ **Critical to efficiently distribute disaster notification and critical rescue information**

Key Use Cases (High-Level)

- Authorities would like to inform citizens of possible shelters, food, or 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

Key Research Challenges

- **Communication in Fragmented Networks** (using disconnected but functional parts of the infrastructure)
- **Security** (access control, message authentication)
- **Traffic Prioritization / Handling Congestion** (overall capacity is reduced)
- **Delay/Disruption Tolerant Approach**
- **Energy Efficiency** (devices run on battery)



How ICN can be Beneficial[1,2]

- **Routing-by-Name**
  - In fragmented networks, references to location-based, fixed addresses may not work as a consequence of disruptions (e.g. reachability of DNS servers)
- **Content-based Access Control**
  - ICN security model can regulate access to data objects (e.g. only to a specific user or class of users) by means of content-based security
- **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
- **Caching**
  - Caching 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)
- **Sessionless Communication**
  - ICN does not require full end-to-end connectivity (facilitating a seemless aggregation between normal operations and a disaster)

[1] J. Seedorf et al.: “Using ICN in disaster scenarios”, draft-irtf-icnrg-disaster-09, IRTF ICNRG, Dec. 2019
[2] J. Seedorf et al.: “The Benefit of Information Centric Networking for Enabling Communications in Disaster Scenarios”, Globecom 2015 Workshop on Information Centric Networking Solutions for Real World Applications (ICNSRA), San Diego, USA, December, 2015

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

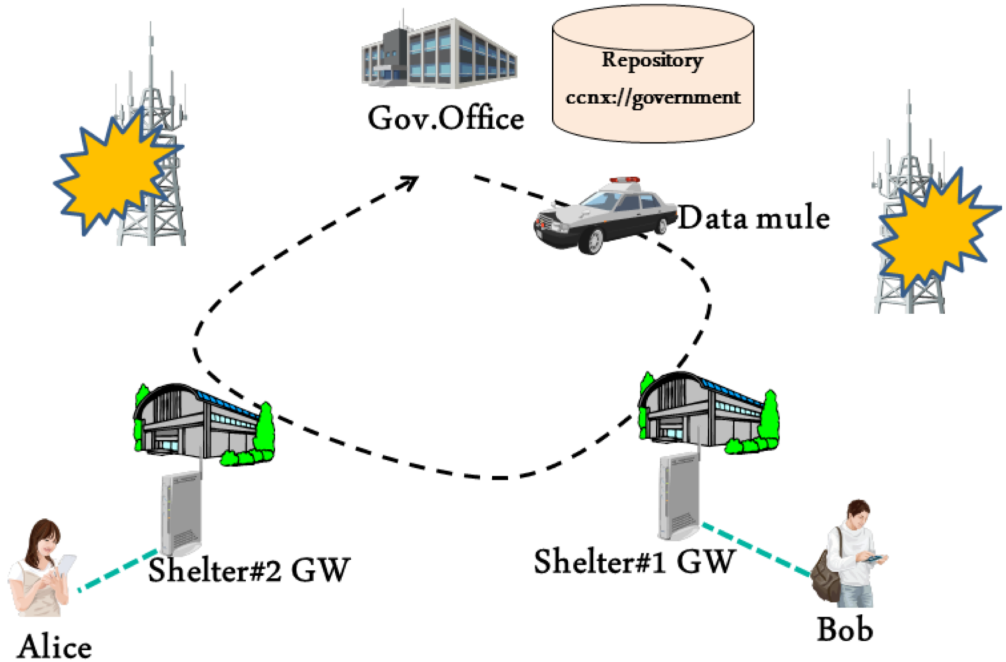
→ Vision / Rationale: Start with existing ICN approaches and extend them with the necessary features needed in disaster scenarios

Hochschule
für Technik
Stuttgart

Overview on selected Solutions

Selected Results

- **ICN 'Data Mules' [2] [3]**
  - Logical interface, multipath support



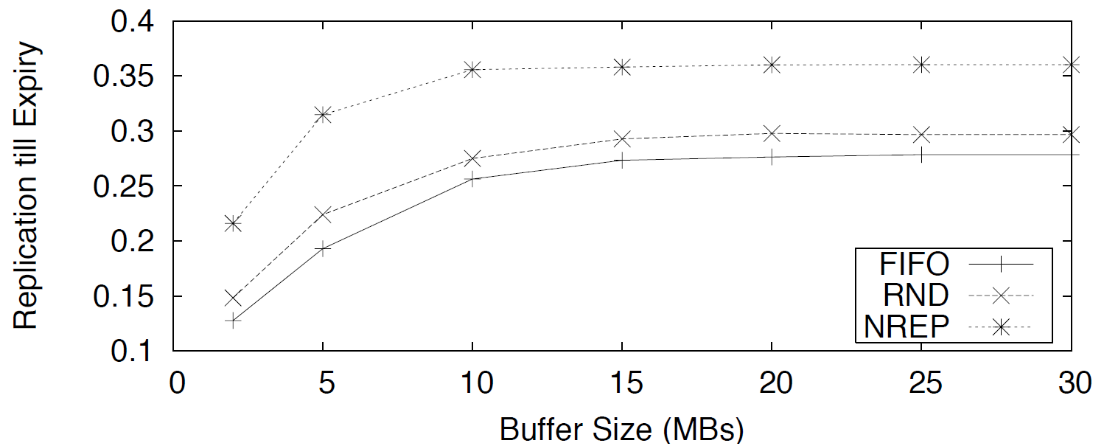
ICN Data Mules in a Disaster Scenario

[2] T. Yagyu and S. Maeda, "Demo Overview: Reliable Contents Retrieval in Fragmented ICNs for Disaster Scenario," ACM ICN Conf., Sep. 2014.
[3] K. Sugiyama et al., "Multipath Support for Name-based Information Dissemination in Fragmented Networks," ACM ICN Conf., Sep./Oct. 2015.

Selected Results

- **ICN 'Data Mules'**

- **Priority dependent Name-based Replication (NREP) [4]**
  - Routing/forwarding decisions based on name/attributes
  - E.g. attaching priority & time/space restrictions to interests



More Replications till Expiry for High Priority Messages

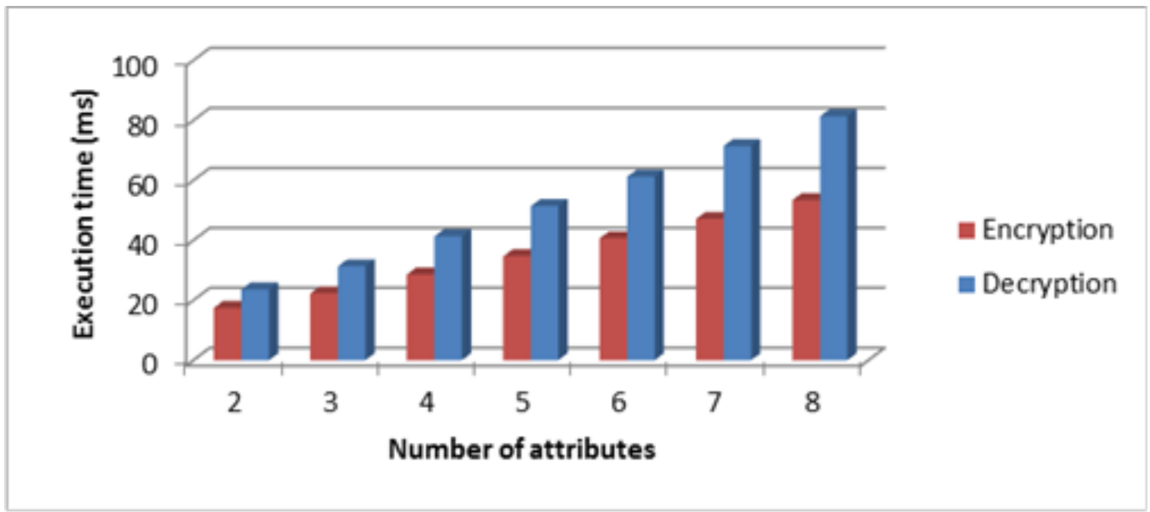
[4] I. Psaras et al., "Name-based replication priorities in disaster cases," in 2nd Workshop on Name Oriented Mobility NOM), 2014.

Selected Results

- ICN 'Data Mules
- Priority dependent Name-based Replication (NREP)
- **Data-centric Confidentiality/Access Control**/Authentication **[5]**
  - Multi-authority 'Ciphertext-Policy Attribute Based Encryption' ICN security architecture
  - Example Policy: allow access only to recipients who fulfill:

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

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



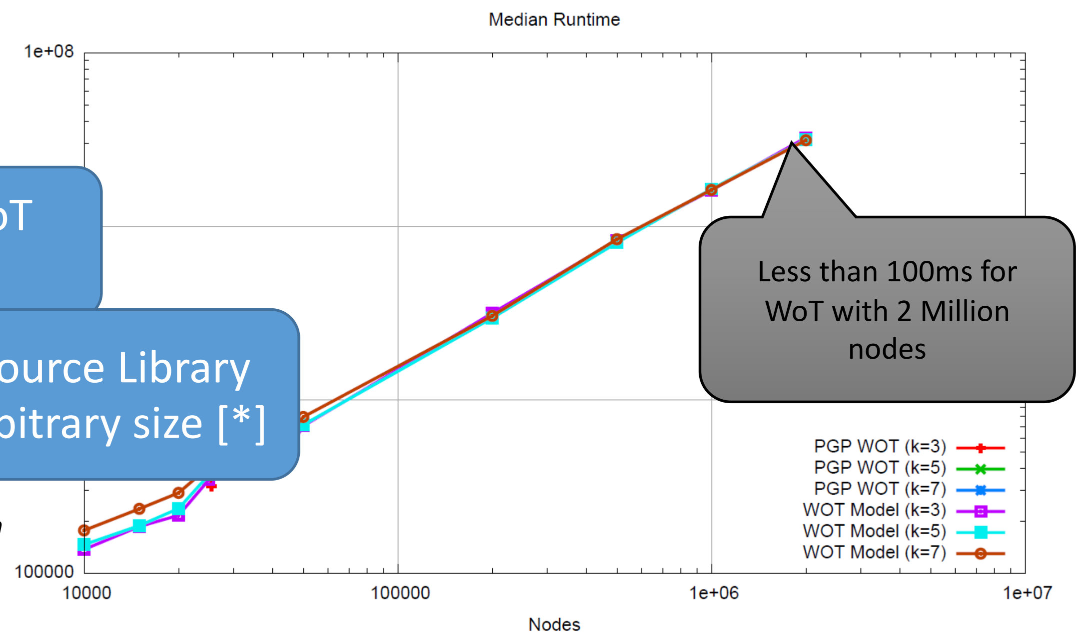
[5] T. Asami et al., "D2.3.1 - initial solution for access control and management in fragmented networks," GreenICN Project, GreenICN Project Deliverable, 2013

Selected Results

- **ICN 'Data Mules'**
- **Priority dependent Name-based Replication (NREP)**
- **Data-centric Confidentiality/Access Control/Authentication [6][7]**
  - Binding between self-certifying ICN names and Real-World Identities via a Web-of-Trust (WoT)
  - Assessing information received based on trust metric executed on the WoT graph

Key idea: Nodes store complete WoT graph in a compressed format

Contribution: Model and Open Source Library for synthesizing WoT graphs of arbitrary size [*]



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

[6] 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

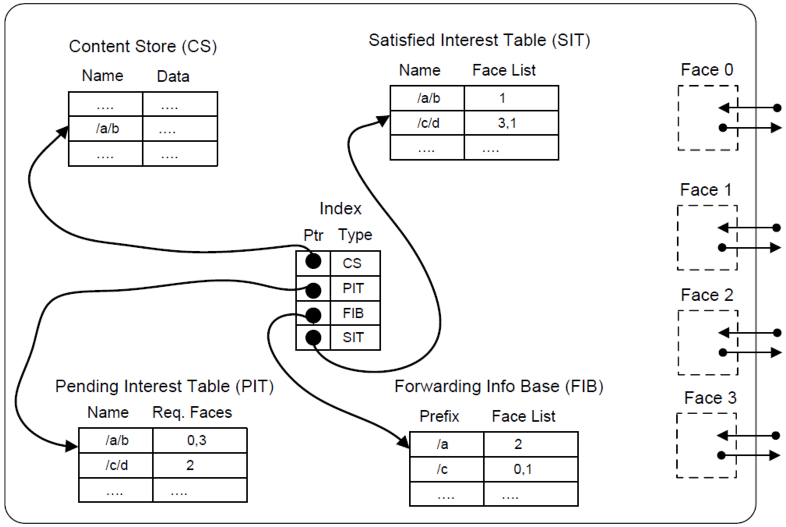
[7] J. Seedorf et al.: "Demo overview: Fully decentralised authentication scheme for icn in disaster scenarios (demonstration on mobile terminals)," in 1st ACM Conference on Information-Centric Networking (ICN-2014), 2014.

[*] https://github.com/BenjaminSchiller/GTNA/tree/master/src/gtna

Selected Results

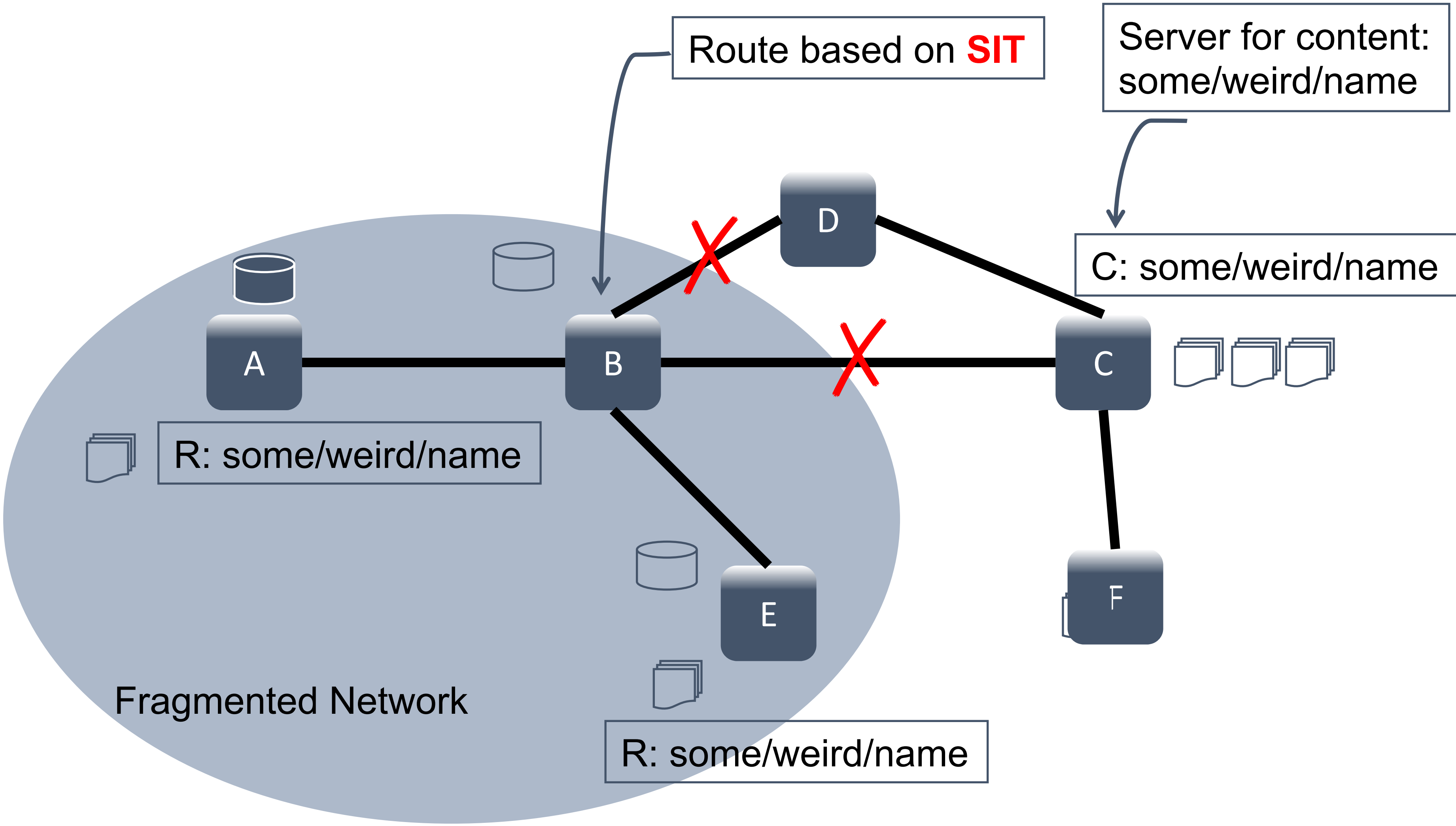
- ICN ’Data Mules’
- Priority dependent Name-based Replication (NREP)
- Data-centric Confidentiality, Access Control, Authentication
- **Information Resilience [8]**
  - NDN Extension “Satisfied Interest Table (SIT)”
  - Keeps track of data packet next hop, i.e. stores info reg. downstream delivery of content
  - Use of this additional routing table in case upstream routing of interests provides no data

Information Resilience: Router Design with Satisfied Interest Table (SIT)



[8] V. Sourlas et al. “Information Resilience through User-Assisted Caching in Disruptive Content-Centric Networks”, IFIP Networking 2015, May 2015

Information Resilience through SIT



Hochschule für Technik Stuttgart

Deep Dive:
Decentralised ICN Interest Popularity Estimation

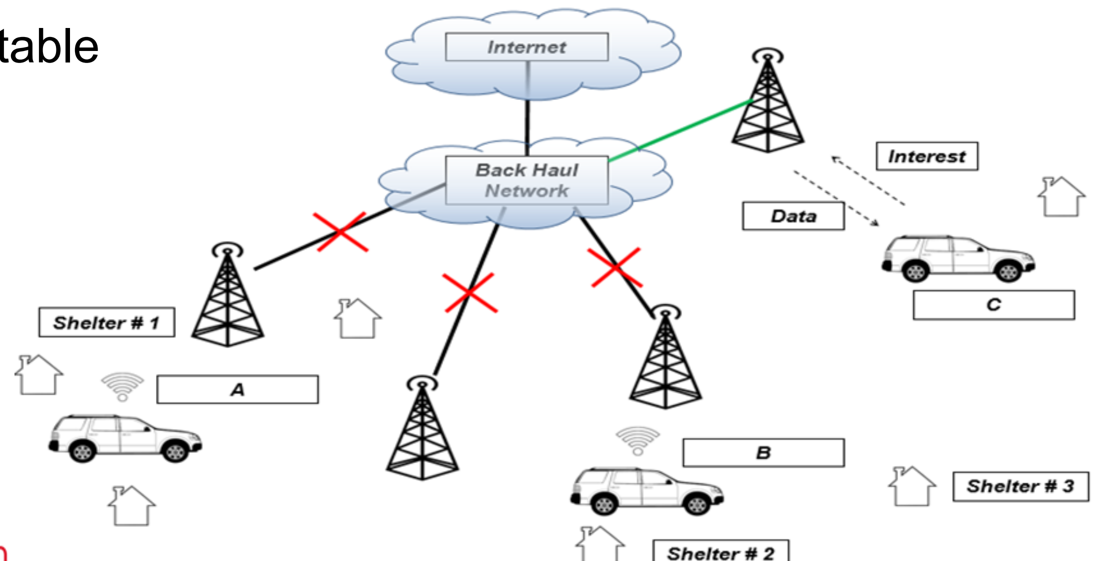
Background & Scope

Background: Disaster Scenario

- GreenICN Project: Using ICN for Disaster Scenarios
- Nodes may be scattered across different fragmented networks
- DTN-like communication using ICN data mules

Goal: Decentralised Popularity Estimation of Interest Messages

- Scenario: ICN data mules with limited storage capabilities and possibly limited delivery time
- Assumption: random, unpredictable movements of ICN data mules
- Date mules need to prioritize ICN messages
- Knowing interest popularity can be an important factor in prioritization



Proposed Solution: Rationale & Overview

General Idea

- Exploit Nonces in ICN Protocols for counting interests received
- Naïve Approach: Append to each end-user request a unique nonce
  - Data mules would need to keep all nonces received in order not to ***over-count*** when encountering again the same end user or data mule in the future
  - Accurate estimation, but clearly does not scale …

Overview of our Proposed Solution

- Idea: Aggregate ***[nonce:counter]*** tuples
  - Approximate content popularity
  - Much more scalable (with respect to memory requirements at nodes)
- General Scheme:
  - End-users assign random nonces to interests
  - Data mules maintain list of [nonce:counter] tuple per interest for scalability
  - When two data mules meet, they exchange their Interests (incl. [nonce:counter])
    - Interests & popularity estimation gets distributed in network

Proposed Solution: Rationale & Overview

Algorithm

- When two data mules encounter each other and both have for a given name already a [nonce:counter] tuple, aggregation of nonces and counters is performed
- For each Interest, aggregate [nonce:counter] tuples as follows:

```
Compare([nonce1, count1] , [nonce2, count2])

IF nonce1 == nonce2
  • new_count = MAX(count1, count2) (at both nodes)

IF nonce1 != nonce2
  • New_nonce = nonce with largest counter([nonce1,
    count1],
    [nonce2, count2])
  • New_count = count1 + count2
```

Hochschule
für Technik
Stuttgart

Proposed Solution: Loop Prevention

Handling Repeated Data Mule Encounters over Time

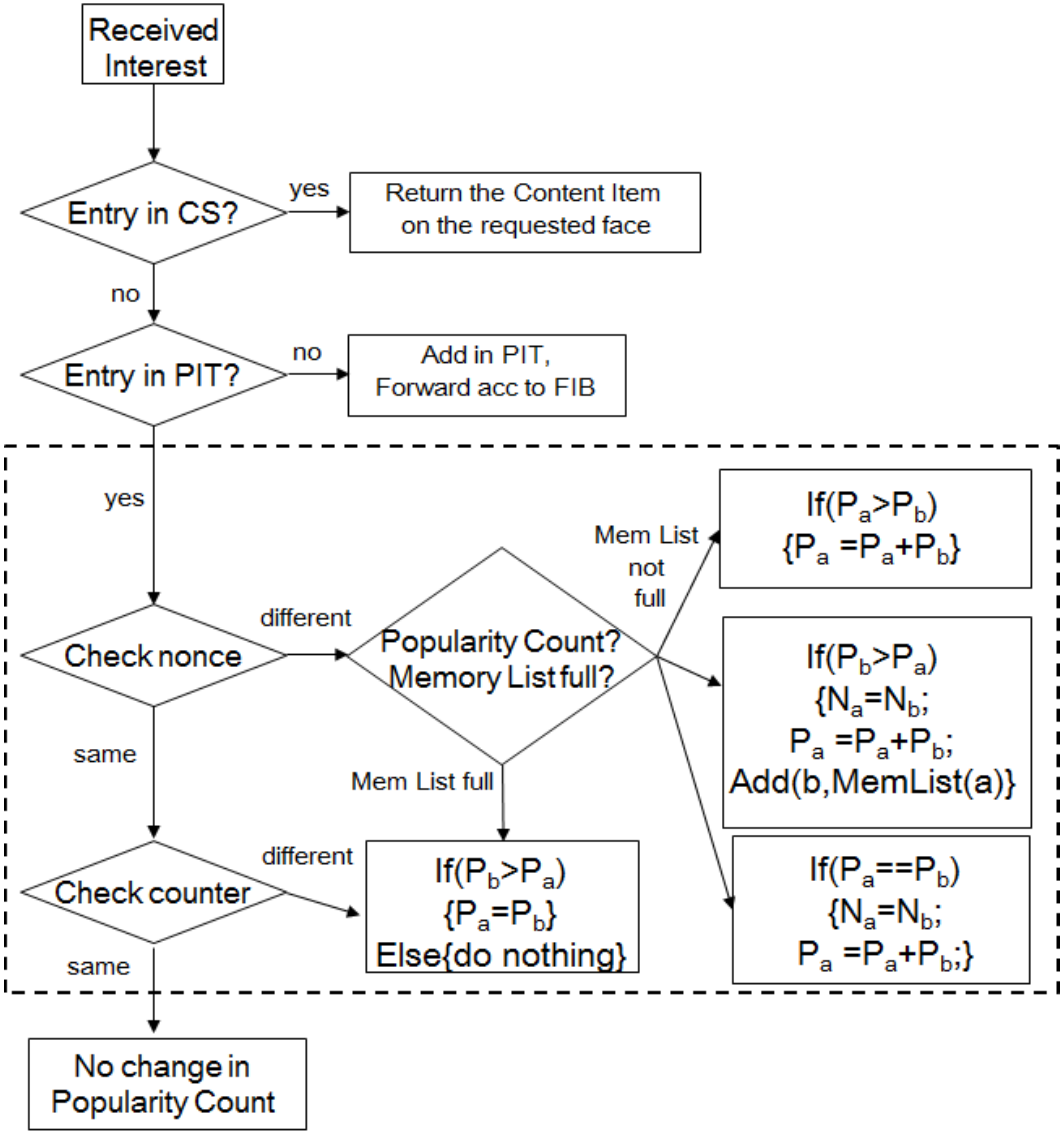
- Memory list: Data mules keep list of recently encountered mules per Interest
- If a data mule is encountered again, counters are not added
- Instead, max-counter rules is applied at both sides:

```
● nonce1 != nonce2 (AND recently met)
    • New_nonce = nonce with largest counter([nonce1,
      count1], [nonce2, count2])
    • New_count = MAX(count1, count2)
```

Limited Memory List Size

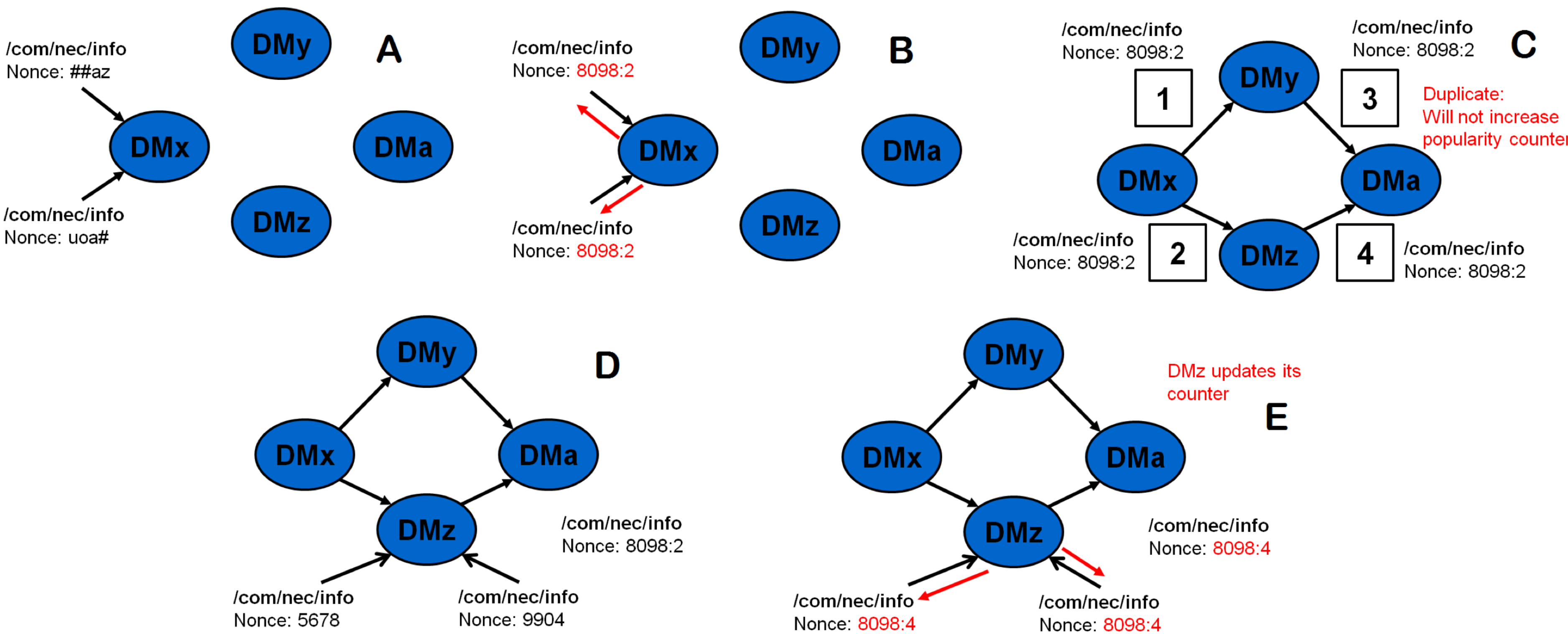
- Memory list of encountered nodes has limited (configurable) size
  - Can trade off accuracy (in popularity-prediction) against memory requirements at nodes
- When memory list full always use max-counter rule:
  `New_count = MAX(count1, count2)` (=treat as if recently met)
- Alternative: Sliding approach = FIFO list of encountered nodes

Proposed Solution: Algorithm

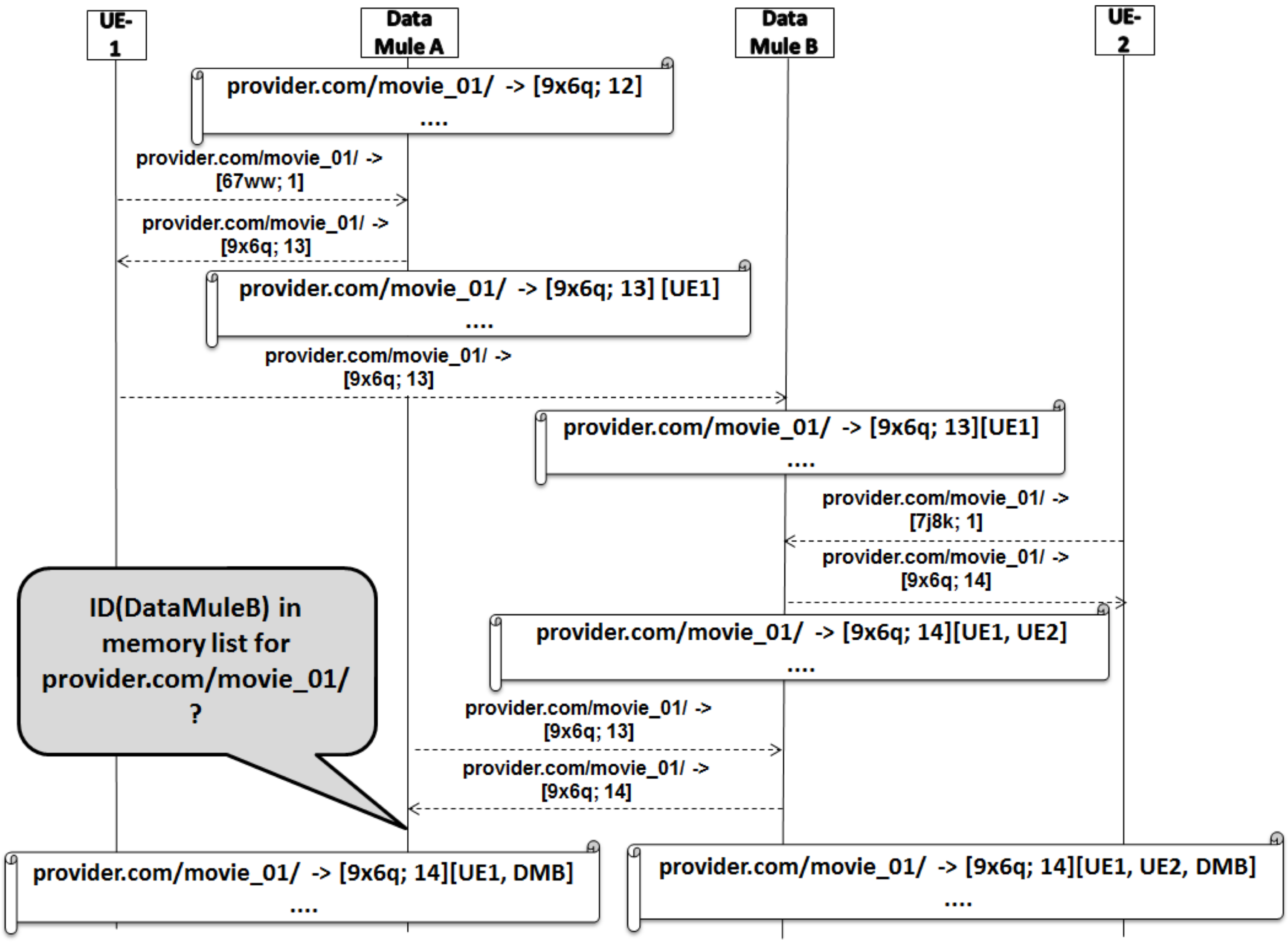


- Data mule a encountering data mule b
- P_a, P_b: popularity counter at data mule a, b
- N_a, N_b: nonce at data mule a, b

Proposed Solution: Nonce Assignment Example



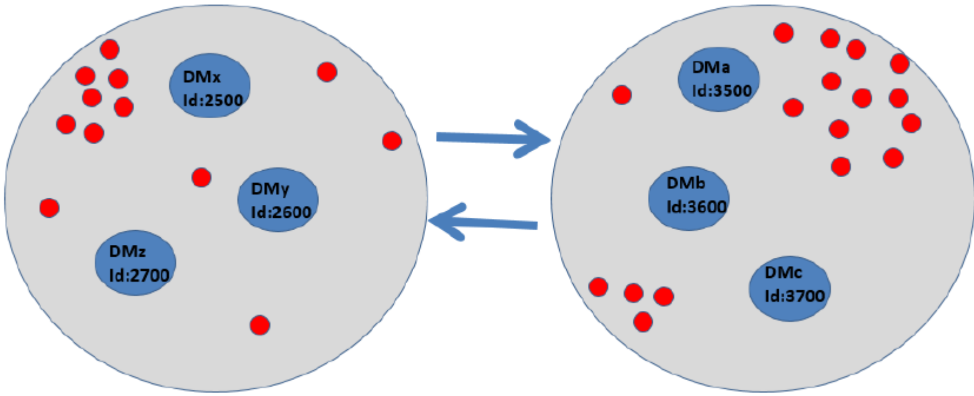
Proposed Solution: Message Flow Example



Evaluation

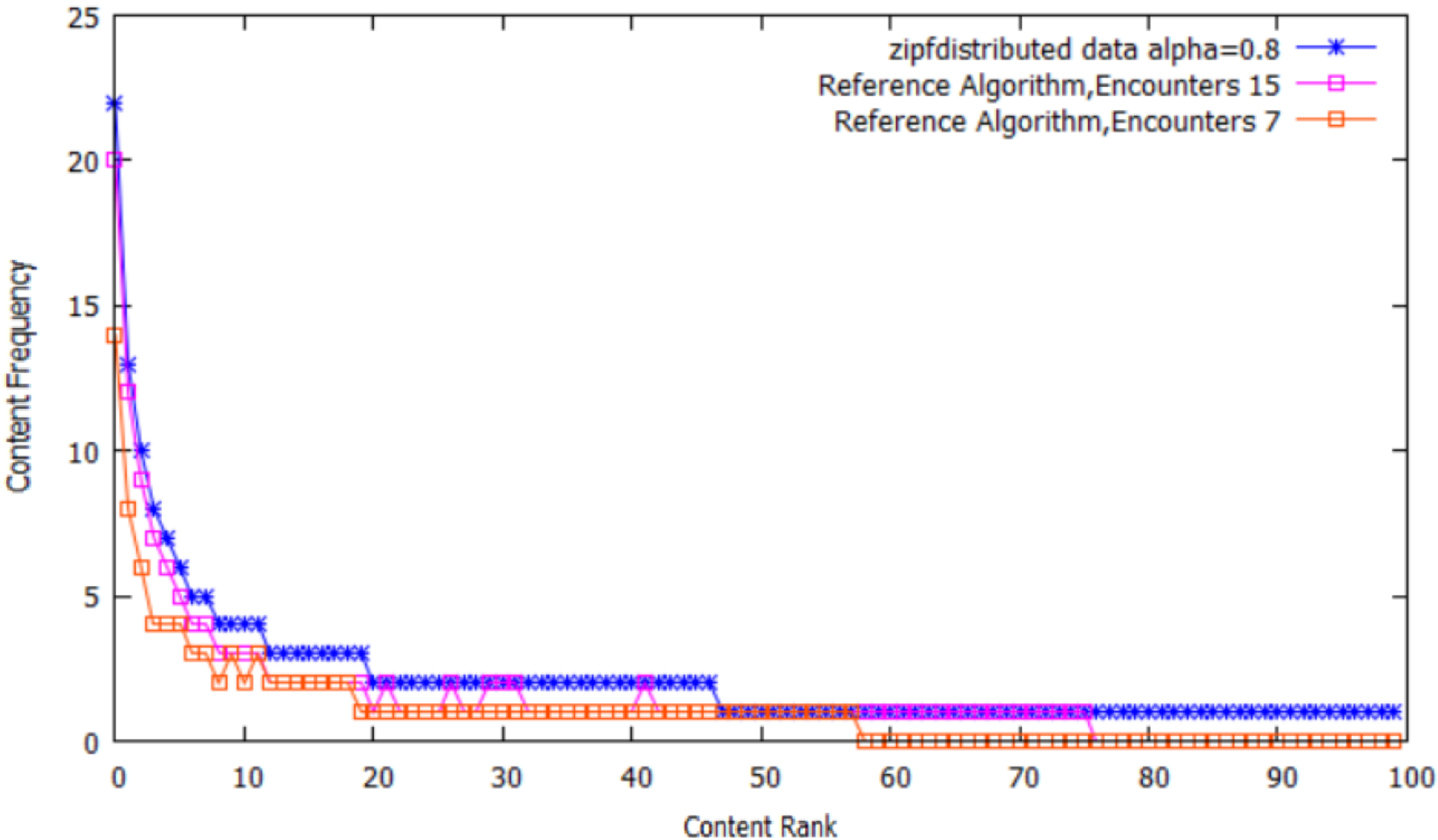
Simulations

- Objective: Evaluate accuracy of distributed popularity estimation
- Reference Algorithm: Naive solution
  - Append to each end-user request a unique nonce
  - At data mule encounters a complete list of nonces is exchanged for every given name in the Pending Interest Table (PIT) of each data mule
- Scenario / Experiments
  - 2 Fragmented Communities with 100 distinct data objects (size: 8kb)
  - Zipf distribution for Interests with 0.8 < alpha <0.9 (appr. 500 interests issued by users)
  - Phase 1
    - 3 different data mules in each of the fragmented communities, receiving interests from users at random
  - Phase 2
    - All 6 Data mules meet each other in a random manner and exchange interests (no disruption during intermeeting times)



Evaluation Scenario

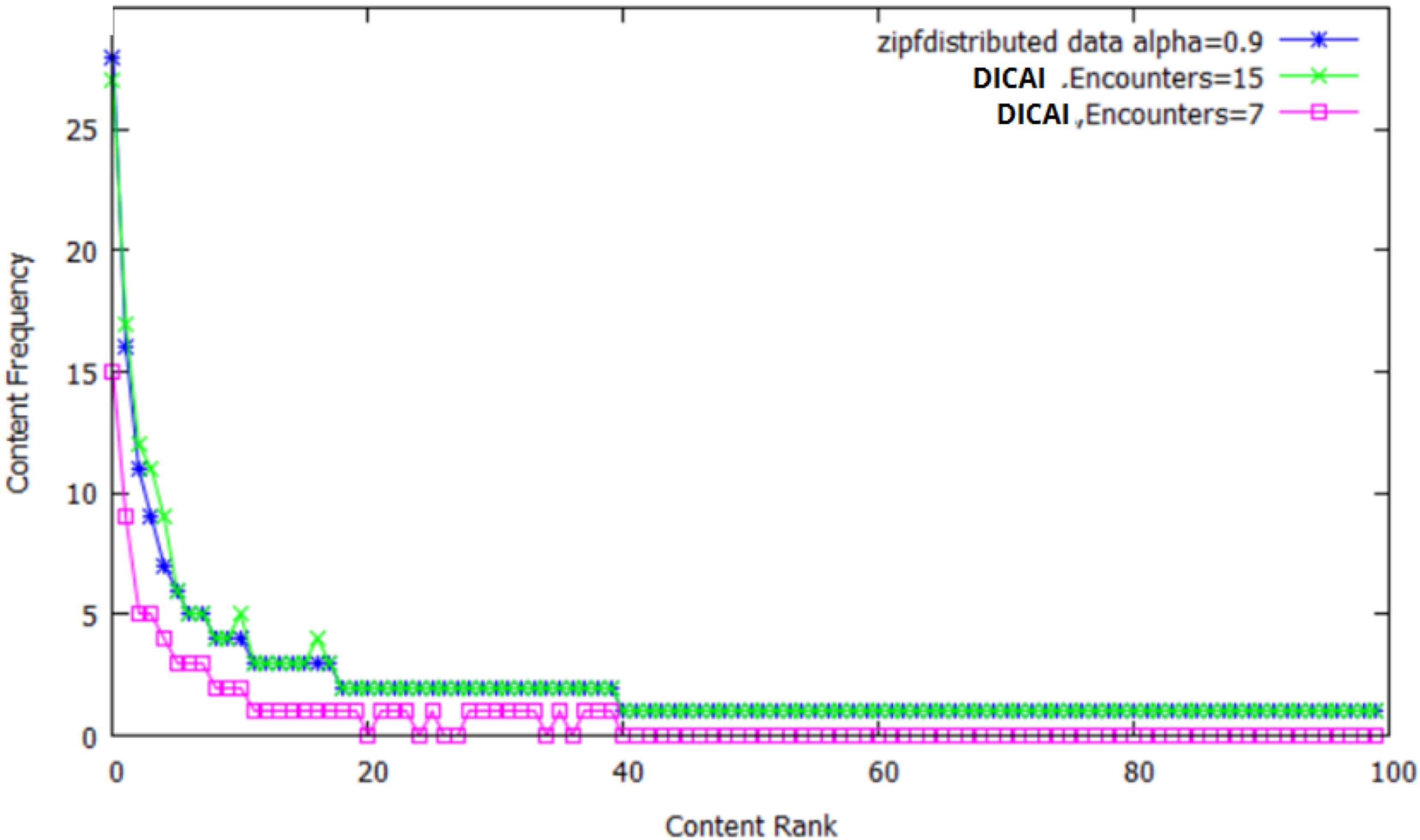
Results: Reference Algorithm



Hochschule
für Technik
Stuttgart

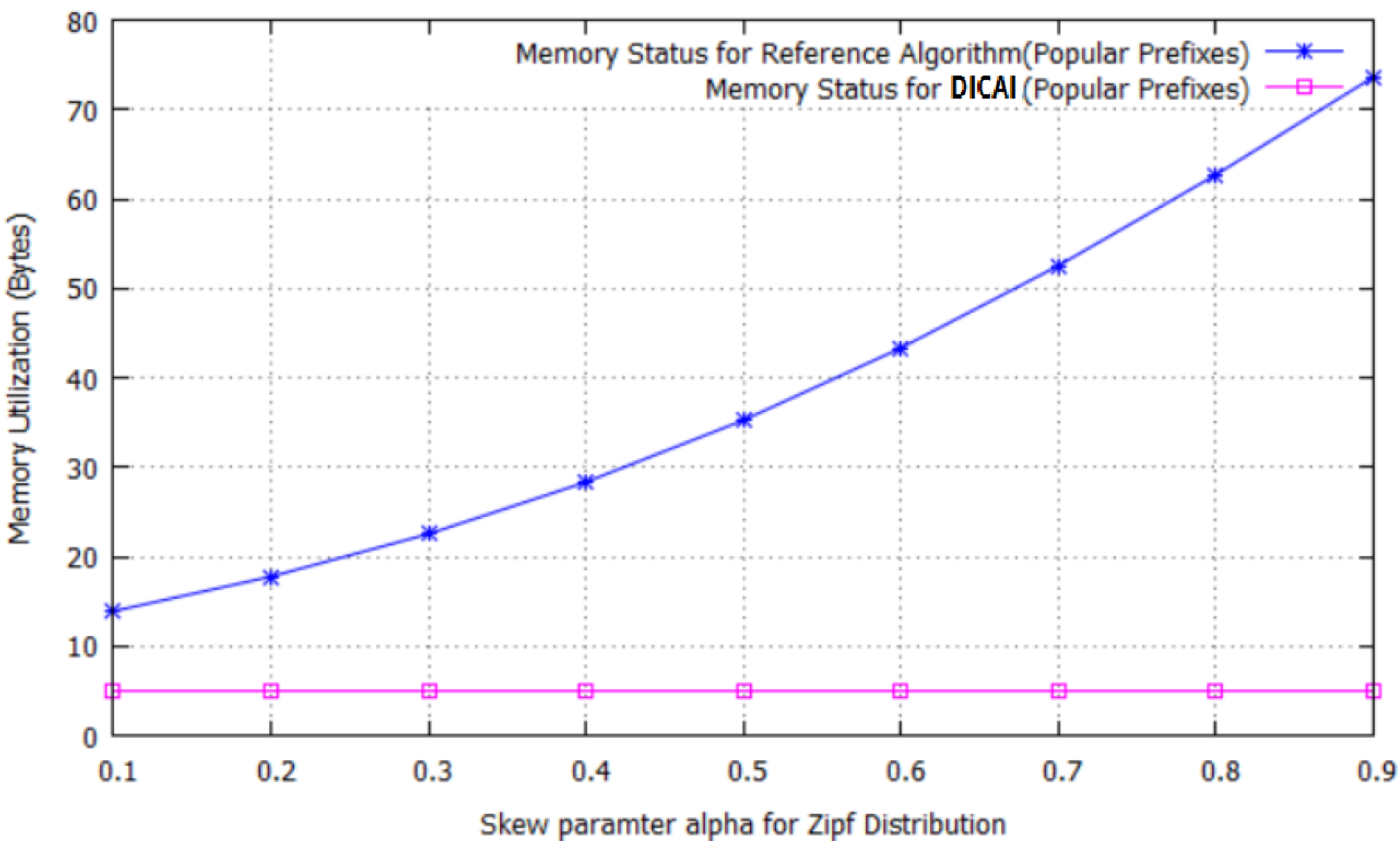
Results: Our Approach

Results for Decentralised Interest Counter Aggregation for ICN (DICAI)



Results: Memory Requirements

Memory utilization for nonces for the top 5 prefixes popularity-wise (among all data mules, 15 encounters, 1 Byte per nonce)



Summary & Contribution

Contribution

- Design of a scalable, fully decentralised scheme for estimating the popularity of ICN interest messages
  - scenario with random, unpredictable movements of ICN data mules
  - very useful to optimize content dissemination after a disaster
- Algorithm described in detail and with concrete examples
- Evaluation
  - Analytical model of the storage overhead introduced by our approach
  - Simulations showing that our proposed solution provides sufficient accuracy in predicting the actual content popularity

Future Work

- More complex simulations
- Actual Implementation (e.g. based on CCNx, NDN)

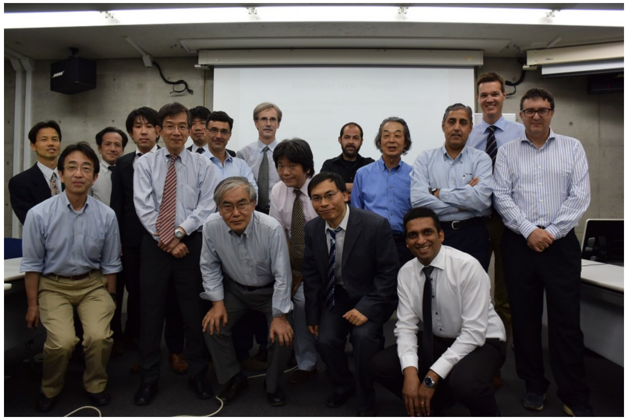
Hochschule
für Technik
Stuttgart

Lessons Learned & Open Questions

ICN is indeed a good match for Disaster Scenarios

Our work confirmed that ICN is a good starting point for enabling disaster aftermath communication

- ICN brings (intrinsicly) many features that are very useful for enabling communications after a disaster happened
  - E.g. naturally supports sessionless communication
- We extended existing ICN approaches with the necessary features needed in disaster scenarios, showing that it is possible to enhance ICN with DTN features
  - Decentralized Forwarding
  - Message Prioritization
  - Security



EU-Japan FP7 GreenICN project successfully completed with a grade of "EXCELLENT"

www.greenicn.org

ICN is indeed a good match for Disaster Scenarios

However, semantics of certain components may change …

- Routing/forwarding essentially changes to a store-carry-forward of interests over a long period of time
  - For some use cases, rather ‘forwarding to anybody’ instead of ‘routing’
- Examples
  - Nonces: Can also be used for interest popularity estimation, and may be aggregated
  - Interest Lifetime: May become more of an application-layer validity-period
  - Faces: Meaning may become somewhat blurry
    - Single physical face (e.g. Wifi) may be used to forward interests to various different nodes over time, independently of their ID (i.e. forward interests to anybody met)
  - Content forwarding: May even be meaningful to exchange popular data items at data mule encounter without a corresponding interest at that point in time

Different Solutions for different Scenarios

- Fixed, predictable movement of ICN Data Mules
  - E.g. forward interests based on logical face
- Semi-random movement of ICN Data Mules (e.g. known direction of rescue teams)
  - E.g. forward interest based on prioritization and/or time/space attributes
- Completely random movement of ICN Data Mules (e.g. end users walking around)
  - E.g. forward interests to anybody based on interest popularity estimation

Security

Disaster Use Case good match for ICN Data-centric Security

- IBE / ABE very suitable for key use cases
- Can assume single trusted key generator (e.g. government, mobile operator) for many use cases
- But may be difficult to apply these approaches on a world-wide scale
  - E.g. scalability / performance of ABE depends on number of attributes
  - Single trusted entity as PKG …

Web-of-Trust fits well the decentralised nature of disaster scenario

- Enables fully decentralised authentication of content
- Our solution is based on self-certifying names (name contains the hash of the public key of the owner of the name)
- WoT provides only trustworthiness for a given name
  - Trust content based on relationships in the WoT graph

➢ Fully decentralised, but more-or-less ‘probabilistic’ security

Security

Name Assignment Responsibility / Ownership of Names

- For hash-based names need to know the hash
  - If name contains hash of content, need to know the correct hash
  - If name contains hash of public key (of the owner of the name), need to know the corresponding Real-World Identity or public key
- Brings up the larger questions of how user obtains names
  - Outside the ICN layer?
  - Via trusted Search Engine?
  - Lengthy discussions ...
- For many of our solutions, just assumed pre-configured or well-known names
  - E.g. within the disaster app on your smartphone
  - E.g. bootstrap via well-known name where other producers can post names under which new content is available (like an ‘alert bulletin board‘)
- May be very use case specific

Other Open Issues

Selected Open Issues*

- Specifying for each mechanism suggested to what exact extent ICN deployment in the network and at user equipment is required
- How to best use DTN and ICN approaches for an optimal overall combination of techniques?
- How do data-centric encryption schemes scale and perform in large- scale, realistic evaluations?
- How to properly disseminate authenticated object names to nodes (for decentralised integrity verification and authentication) before a disaster, or how to retrieve new authenticated object names by nodes during a disaster?

*See further: J. Seedorf et al.: “Research Directions for Using ICN in Disaster Scenarios“
https://tools.ietf.org/html/draft-irtf-icnrg-disaster

Hochschule
für Technik
Stuttgart

Questions & Discussion ...