Empowered by Innovation NEC

Fully Decentralised Authentication Scheme for ICN in Disaster Scenarios (Demonstration on Mobile Terminals)

Jan Seedorf, Bilal Gill, and Dirk Kutscher
NEC Laboratories Europe

Benjamin Schiller and Dirk Kohlweyer
Technical University of Darmstadt

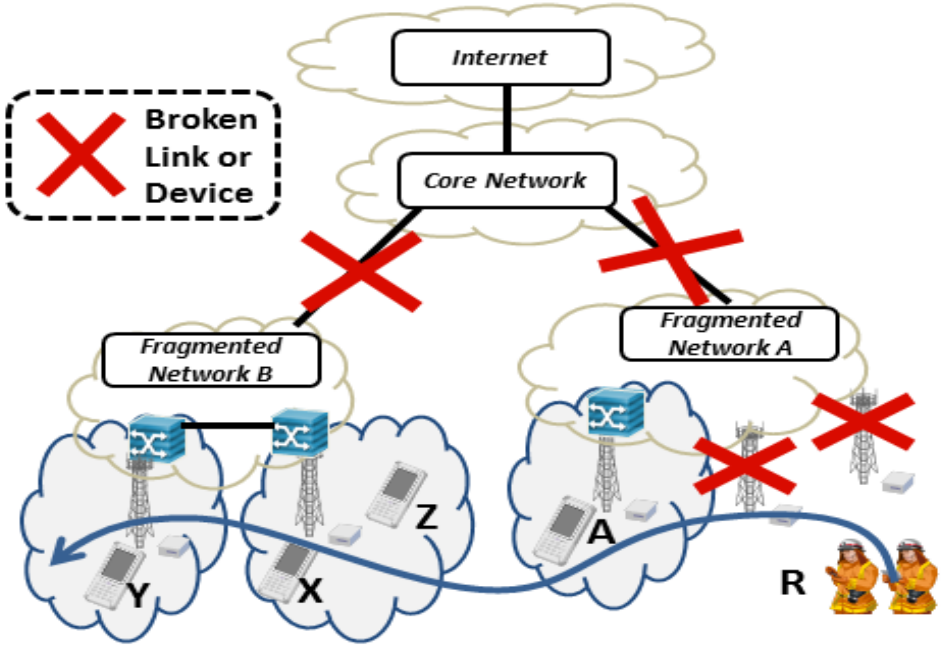
Contact: Jan.seedorf@neclab.eu

IETF-91
Honolulu, Hawaii, USA

Scenario and Use Case

Disaster Scenario

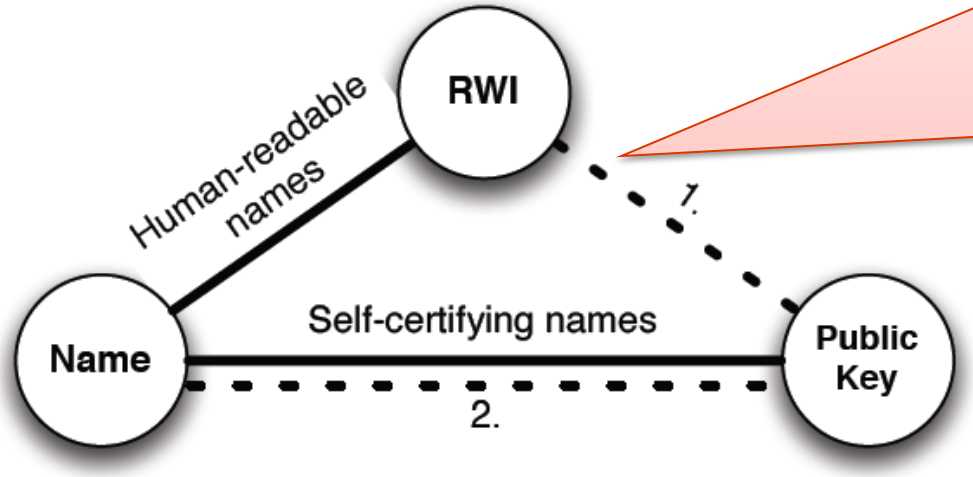
- The aftermath of a disaster, e.g. hurricane, earthquake, tsunami, or a human-generated network breakdown
- E.g. the enormous earthquake which hit Northeastern Japan on March 11, 2011 (causing extensive damages including blackouts, fires, tsunamis and a nuclear crisis)



Objective: Message Authentication

- Assuming that a message can somehow be delivered across fragmented networks (via content-oriented, DTN-like mechanisms), Y still needs to be able to verify that a message published by Z is trustworthy
- E.g. for “Assessing Warnings“ published by citizens

Challenge: Binding in Naming Schemes*



Our Scheme:
Using a Web-of-Trust in a Decentralised Fashion to Provide this Binding

(Decentralised = No Connectivity to any kind of server needed)

Figure 1: A depiction of the three entities and the different bindings between them. Two naming schemes provide different intrinsic bindings (solid lines) but require both an external authority to provide one additional binding (dashed line): with self-certifying names it's the binding (1), whereas with human-readable names it's the binding (2).

**Ghodsi et al: "Naming in Content-Oriented Architectures", SIGCOMM ICN Workshop 2011*

High-Level Overview of Scheme *

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

**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*

Demo Overview

Implementation

- Developed a methodology to synthesize large-scale WoT-graphs
  - maintaining several key graph theoretic properties as prevalent in the PGP Web-of-Trust (degree distribution, path length distribution, …)
  - implemented this WoT-model in the JAVA-based Graph-Theoretic Analysis Framework (GTNA)*
- Implemented a dBFS-algorithm
  - for finding certificate chains on WoT-graphs
- Implemented several trust metrics
  - shortest certificate chain found
  - number of certicate chains found with maximum length

Demo: Running on Android

- Pre-loaded WoT-files of different size
- User can select a) WoT-size, b) trust metric, c) parameters for trust metric
- Shows runtime of selection when choosing two users in the WoT randomly, thus showing
  - how the dBFS algorithm scales with increasing WoT sizes
  - how the dBFS algorithm scales depending on trust metric
  - how it would perform on common smartphones

**https://www.p2p.tu-darmstadt.de/research/gtna/*

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.

APPENDIX

High-Level Research Challenges*

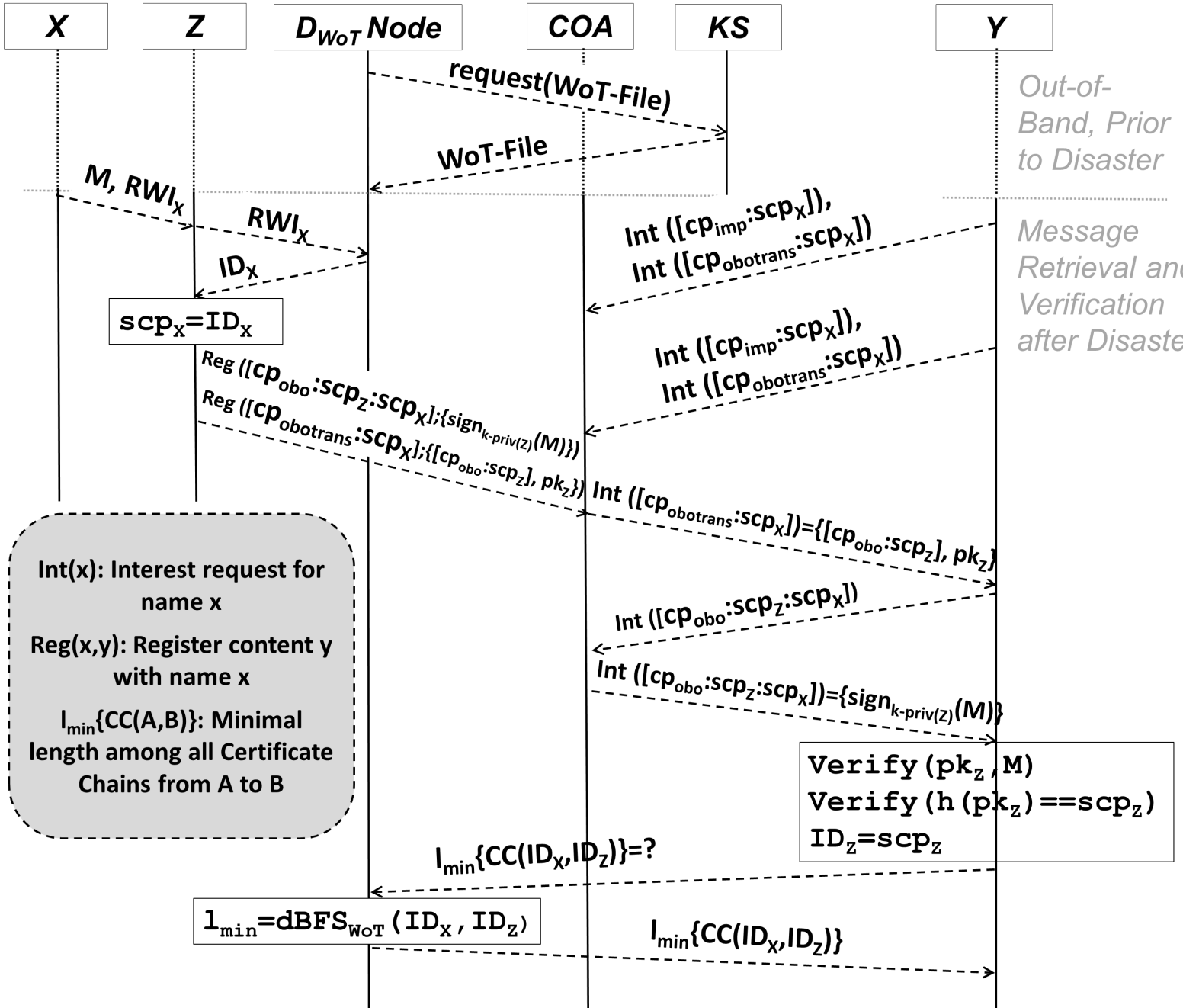
- Enabling usage of functional parts of the infrastructure, even when these are disconnected from the rest of the network
- Delivering/obtaining information in (highly) congested networks
- Decentralised authentication
  - In today's mobile networks, users are authenticated via central entities
  - In 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)

Existing Solutions Assumed

Focus of this Demo

**See further M. Arumaithurai, J. Seedorf, et. al: "Using ICN in disaster scenarios", draft-seedorf-icn-disaster*

Detailed Scheme



Analytical Estimation of Time & Space Needed

Time and Space Requirements for Graph Search

$$t(dBFS) = 2 \times \left(b^{\frac{d}{2}} + b^{\frac{d}{2}-1} + \ldots + b \right)$$

$$s(dBFS) = m_{req}(node) \times 2 \times \left(b^{\frac{d}{2}} + b^{\frac{d}{2}-1} + \ldots + b \right)$$

- b: branching factor; d: the depth of the search
- In our case: d is the certificate path length and b is the average number of identities a member of the WoT has signed
- m_{req}(node) refers to the space needed for storing a single node (i.e. as graph vertex) in memory

Size of Compressed Certificate Graph

$$size(f_{wot}) = n \times (m_{req}(name))_{av} + n \times m_{req}(node) + n \times b \times m_{req}(node)\ [byte]$$

- n: total number of nodes (i.e. real-world identities) in the WoT
- $m_{req}(name)_{av}$: average space needed for storing a real-world identity

Empowered by Innovation