ICNRG M. Arumaithurai
Internet-Draft J. Seedorf
Intended status: Informational NEC
Expires: January 16, 2014 A. Tagami
KDDI R&D Labs
K. Ramakrishnan
AT&T
N. Blefari Melazzi
Univ. Tor Vergata
July 15, 2013

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

Abstract

Information Centric Networking is a new paradigm where the network provides users with named content, instead of communication channels between hosts. This document outlines some research directions for Information Centric Networking (ICN) with respect to applying ICN approaches for coping with natural or human-generated, large-scale disasters.

Table of Contents

1. Introduction

This document summarizes some research challenges for coping with natural or human-generated, large-scale disasters. Further, the document discusses potential directions for applying Information Centric Networking (ICN) to address these challenges.

Section 2 gives some examples of what can be considered a large-scale disaster and what the effects of such disasters on communication networks are. Section 3 outlines why ICN can be beneficial in such scenarios and provides a high-level overview on corresponding research challenges. Related research activities are ongoing in the GreenICN research project; Section 4 provides an overview of this project.

2. Disaster Scenarios

An enormous earthquake hit Northeastern Japan (Tohoku areas) on March 11, 2011, and caused extensive damages including blackouts, fires, tsunamis and a nuclear crisis. The lack of information and means of communication caused the isolation of several Japanese cities. This impacted the safety and well-being of residents, and affected rescue work, evacuation activities, and the supply chain for food and other essential items. Even in the Tokyo area that is 300km away from the Tohoku area, more than 100,000 people became 'returner' refugees, who could not reach their homes because they had no means of public transportation (the Japanese government has estimated that more than

6.5 million people would become returner refugees if such a catastrophic disaster were to hit the Tokyo area). This recent earthquake in Northeastern Japan also showed that the current network is vulnerable against disasters and that mobile phones have become the lifelines for communication including safety confirmation. The aftermath of a disaster puts a high strain on available resources due to the need for communication by everyone. Authorities such as the President/Prime-Minister, local authorities, Police, fire brigades, and rescue and medical personnel 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. Moreover, damage to communication equipment, in addition to the already existing heavy demand for communication highlights the issue of fault-tolerance and energy efficiency.

Additionally, disasters caused by humans such as a terrorist attack need to be considered, i.e. disasters that are caused deliberately and willfully and have the element of human intent. In such cases, the perpetrators could be actively harming the network by launching a Denial-of-Service attack or by monitoring the network passively to obtain information exchanged, even after the main disaster itself has taken place. Unlike some natural disasters that are predictable using weather forecasting technologies and have a slower onset and occur in known geographical regions and seasons, terrorist attacks may occur suddenly without any advance warning. Nevertheless, there exist many commonalities between natural and human-induced disasters, particularly relating to response and recovery, communication, search and rescue, and coordination of volunteers.

3. Research Challenges and Benefits of ICN

3.1. High-Level Research Challenges

Given a disaster scenario as described in Section 2, on a high-level one can derive the following (incomplete) list of corresponding technical challenges:

o Enabling usage of functional parts of the infrastructure, even when these are disconnected from the rest of the network: Assuming that parts of the network infrastructure (i.e. cables/links, routers, mobile bases stations, ...) are functional after a disaster has taken place, it is desirable to be able to continue using such components for communication as much as possible. This is challenging when these components are disconnected from the backhaul, thus forming fragmented networks. This is especially true for today's mobile networks which are comprised of a

centralised architecture, mandating connectivity to central entities (which are located in the core of the mobile network) for communication. But also in fixed networks, access to a name resolution service is often necessary to access some given content.

- Decentralised authentication: In 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 such user authentication arises. Independently of the network being fixed or mobile, 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: Due to broken cables, failed routers, etc., it is likely that in a disaster scenario the communication network has much less overall capacity for handling traffic. Thus, significant congestion can be expected in parts of the infrastructure. It is therefore a challenge to guarantee message delivery in such a scenario. This is 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).

The list above is most likely incomplete; future revisions of this document intend to add additional challenges to the list.

3.2. How ICN can be Beneficial

Several aspects of ICN make related approaches attractive candidates for addressing the challenges described in Section 3.1. Below is an (incomplete) list of considerations why ICN approaches can be beneficial to address these challenges:

- Routing-by-name: ICN protocols natively route by named data objects and can identify devices by names, effectively moving the process of name resolution from the application layer to the network layer. This functionality is 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: ICN is built around the concept of named data objects. Several proposals exist for integrating the concept of 'self-certifying data' into a naming scheme (see e.g. [RFC6920]). With such 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 content along a delivery path is an inherent concept in ICN. 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).

The list above is most likely incomplete; future revisions of this document intend to add more considerations to the list and to argue in more detail why ICN is suitable for addressing the aforementioned research challenges.

4. The GreenICN Project

This section provides a brief overview of the GreenICN project. You can find more information at the project web site http://www.greenicn.org/

The recently formed GreenICN project, funded by the EU and Japan, aims to accelerate the practical deployment of ICN, addressing how ICN networks and devices can operate in a highly scalable and energy-efficient way. The project will exploit the designed infrastructure to support multiple applications including the following two broad exemplary scenarios: 1) The aftermath of a disaster, e.g. hurricane, earthquake, tsunami, or a human-generated network breakdown when energy and communication resources are at a premium and it is critical to efficiently distribute disaster notification and critical rescue information. Key to this is the ability to exploit fragmented networks with only intermittent connectivity, the potential exploitation of multiple modalities of communication and use of query/response and pub/sub approaches; 2) Scalable, efficient pub/sub video delivery, a key requirement in both normal and disaster situations.

GreenICN will expose a functionality-rich API to spur the creation of new applications and services expected to drive industry and consumers, with special focus on the EU and Japanese environments, into ICN adoption. Our team, comprising researchers with diverse expertise, system and network equipment manufacturers, device vendors, a startup, and mobile telecommunications operators, is very

well positioned to design, prototype and deploy GreenICN technology, and validate usability and performance of real-world GreenICN applications, contributing to create a new, low-energy, Information-Centric global communications infrastructure. We also plan to make contributions to standards bodies to further the adoption of ICN technologies.

5. Conclusion

This document outlines some research directions for Information Centric Networking (ICN) with respect to applying ICN approaches for coping with natural or human-generated, large-scale disasters. The document describes high-level research challenges as well as a general rationale why ICN approaches could be beneficial to address these challenges. One main objective of this document is to gather feedback from the ICN community within the IETF and IRTF regarding how ICN approaches can be suitable to solve the presented research challenges. Future revisions of this draft intend to include additional research challenges and to discuss what implications this research area has regarding related, future IETF standardisation.

6. Normative References

[RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, April 2013.

Appendix A. Acknowledgment

This document 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.

Authors' Addresses

Mayutan Arumaithurai
NEC
Kurfuerstenanlage 36
Heidelberg 69115
Germany

Phone: +49 6221 4342 187
Fax: +49 6221 4342 155
Email: arumaithurai@neclab.eu

Jan Seedorf
NEC
Kurfuerstenanlage 36
Heidelberg 69115
Germany

Phone: +49 6221 4342 221
Fax: +49 6221 4342 155
Email: seedorf@neclab.eu

Atsushi Tagami
KDDI R&D Labs
2-1-15 Ohara
Fujimino, Saitama 356-85025
Japan

Phone: +81 49 278 73651
Fax: +81 49 278 7510
Email: tagami@kddilabs.jp

K. K. Ramakrishnan
AT&T
180 Park Ave
Florham Park NJ 07932
USA

Email: kkrama@research.att.com

Nicola Blefari Melazzi
Univ. Tor Vergata
Via del Politecnico, 1
Roma 00133
Italy

Phone: +39 06 7259 7501
Fax: +39 06 7259 7435
Email: blefari@uniroma2.it