

ICNRG
Internet-Draft
Intended status: Informational
Expires: September 4, 2015

J. Seedorf
NEC
M. Arumaithurai
University of Goettingen
A. Tagami
KDDI R&D Labs
K. Ramakrishnan
University of California
N. Blefari Melazzi
University Tor Vergata
March 3, 2015

Using ICN in disaster scenarios
draft-seedorf-icn-disaster-03

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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 4, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Disaster Scenarios	3
3. Research Challenges and Benefits of ICN	4
3.1. High-Level Research Challenges	4
3.2. How ICN can be Beneficial	5
4. Use Cases and Requirements	6
5. Solution Design	7
6. The GreenICN Project	9
7. Conclusion	10
8. References	10
8.1. Normative References	10
8.2. Informative References	10
Appendix A. Acknowledgment	11
Authors' Addresses	11

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. Section 4 describes some concrete use cases and requirements for disaster scenarios. In Section 5, some concrete ICN-based solutions approaches are outlined. Related research activities are ongoing in the GreenICN research project; Section 6 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).

That earthquake in 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 may 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.

The timely dissemination of information generated and requested by all the affected parties during and the immediate aftermath of a disaster is difficult to provide within the current context of global

information aggregators (such as Google, Yahoo, Bing etc.) that need to index the vast amounts of specialized information related to the disaster. Specialized coverage of the situation and timely dissemination are key to successfully managing disaster situations. We believe that network infrastructure capability provided by Information Centric Networks can be suitable, in conjunction with application and middleware assistance.

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.
- o 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).
- o 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).

- o Delay/Disruption Tolerant Approach: Fragmented networks makes it difficult to support end-to-end communication. However, communication in general and especially during disaster can tolerate some form of delay. E.g. in order to know if his/her relatives are safe or a 'SOS' call need not be supported in an end-to-end manner. It is sufficient to improve communication resilience in order to deliver such important messages.
- o Energy Efficiency: Long-lasting power outages may lead to batteries of communication devices running out, so designing energy-efficient solutions is very important in order to maintain a usable communication infrastructure.

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:

- o Routing-by-name: ICN protocols natively route by named data objects and can identify objects 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). In highly decentralised scenarios (e.g. in infrastructureless, opportunistic environments) the ICN routing-by-name paradigm effectively may lead to a 'replication-by-name' approach, where content is replicated depending on its name.
- o 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.
- o 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.

- o 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).
- o Sessionless: ICN does not require full end-to-end connectivity. This feature facilitates a seamless aggregation between a normal network and a fragmented network, which needs DTN-like message forwarding.

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. Use Cases and Requirements

This Section describes some use cases for the aforementioned disaster scenario (as outlined in Section 2) and discusses the corresponding technical requirements for enabling these use cases.

- o Delivering Messages to Relatives/Friends: After a disaster strikes, citizens want to confirm to each other that they are safe. For instance, shortly after a large disaster (e.g., Earthquake, Tornado), people have moved to different refugee shelters. The mobile network is not fully recovered and is fragmented, but some base stations are functional. This use case imposes the following high-level requirements: a) People must be able to communicate with others in the same network fragment, b) people must be able to communicate with others that are located in different fragmented parts of the overall network. More concretely, the following requirements are needed to enable the use case: a) a mechanism for scalable message forwarding scheme that dynamically adapts to changing conditions in disconnected networks, b) DTN-like mechanisms for getting information from disconnected island to another disconnected island, and c) data origin authentication so that users can confirm that the messages they receive are indeed from their relatives or friends.
- o Spreading Crucial Information to Citizens: State authorities want to be able to convey important information (e.g. warnings, or information on where to go or how to behave) to citizens. These kinds of information shall reach as many citizens as possible.

i.e. Crucial content from legal authorities shall potentially reach all users in time. The technical requirements that can be derived from this use case are: a) Data origin authentication, such that citizens can confirm the authenticity of messages sent by authorities, b) mechanisms that guarantee the timeliness and loss-free delivery of such information, which may include techniques for prioritizing certain messages in the network depending on who sent them, and c) DTN-like mechanisms for getting information from disconnected island to another disconnected island.

It can be observed that different key use cases for disaster scenarios imply overlapping and similar technical requirements for fulfilling them. As discussed in Section 3.2, ICN approaches are envisioned to be very suitable for addressing these requirements with actual technical solutions.

5. Solution Design

This Section outlines some ICN-based approaches that aim at fulfilling the previously mentioned use cases and requirements.

- o ICN 'data mules': To facilitate the exchange of messages between different network fragments, mobile entities can act as ICN 'data mules' which are equipped with storage space and move around the disaster-stricken area gathering information to be disseminated. As the mules move around, they deliver messages to other individuals or points of attachment to different fragments of the network. These 'data mules' could have a pre-determined path (an ambulance going to and from a hospital), a fixed path (drone/robot assigned specifically to do so) or a completely random path (doctors moving from one camp to another).
- o Priority dependent Name-based replication: By allowing spatial and temporal scoping of named messages, priority based replication depending on the scope of a given message is possible. Clearly, spreading information in disaster cases involves space and time factors that have to be taken into account as messages spread. A concrete approach for such scope-based prioritisation of ICN messages in disasters, called 'NREP', has been proposed [Psaras2014], where ICN messages have attributes such as user-defined priority, space, and temporal-validity. These attributes are then taken into account when prioritizing messages. In [Psaras2014], evaluations show how this approach can be applied to the use case 'Delivering Messages to Relatives/Friends' described in Section 4

- o Energy Efficiency: A large-scale disaster causes a large-scale blackout and thus a number of base stations (BSs) will be operated by their batteries. Capacities of such batteries are not large enough to provide cellular communication for several days after the disaster. In order to prolong the batteries' life from one day to several days, different techniques need to be explored: Priority control, cell-zooming, and collaborative upload. Cell zooming switches-off some of the BSs because switching-off is the only way to reduce power consumed at the idle time. In cell zooming, areas covered by such inactive BSs are covered by the active BSs. Collaborative communication is complementary to cell zooming and reduces power proportional to a load of a BS. The load represents cellular frequency resources. In collaborative communication, end-devices delegate sending and receiving messages to and from a base station to a representative end-device of which radio propagation quality is better. The design of an ICN-based publish/subscribe protocol that incorporates collaborative upload is ongoing work. In particular, the integration of collaborative upload techniques into the COPSS (Content Oriented Publish/Subscribe System) framework is envisioned [COPSS2011].
- o Data-centric confidentiality and access control: In ICN, the requested content is not anymore associated to a trusted server or an endpoint location, but it can be retrieved from any network cache or a replica server. This call for 'data-centric' security, where security relies on information exclusively contained in the message itself, or, if extra information provided by trusted entities is needed, this should be gathered through offline, asynchronous, and non interactive communication, rather than from an explicit online interactive handshake with trusted servers. The ability to guarantee security without any online entities is particularly important in disaster scenarios with fragmented networks. One concrete cryptographic technique is '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. Such encryption schemes tie confidentiality and access-control to the transferred data, which can be transmitted also in an unsecured channel, enabling the source to specify the set of nodes allowed to decrypt.
- o Decentralised authentication of messages: Self-certifying names provide the property that any entity in a distributed system can verify the binding between a corresponding public key and the self-certifying name without relying on a trusted third party. Self-certifying names thus provide a decentralized form of data origin authentication. However, self-certifying names lack a binding with a corresponding real-world identity. Given the

decentralised nature of a disaster scenario, a PKI-based approach for binding self-certifying names with real-world identities is not feasible. Instead, a Web-of-Trust can be used to provide this binding. Not only are the cryptographic signatures used within a Web-of-Trust independent of any central authority; there are also technical means for making the inherent trust relationships of a Web-of-Trust available to network entities in a decentralised, 'offline' fashion, such that information received can be assessed based on these trust relationships. A concrete scheme for such an approach has been published in [Seedorf2014], where also concrete examples for fulfilling the use case 'Delivering Messages to Relatives/Friends' with this approach are given.

6. 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.

7. 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.

8. References

8.1. 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.

8.2. Informative References

[COPSS2011]
Chen, J., Arumaithurai, M., Jiao, L., Fu, X., and K. Ramakrishnan, "COPSS: An Efficient Content Oriented Publish/Subscribe System", Seventh ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), 2011, .

[Psaras2014]
Psaras, I., Saino, L., Arumaithurai, M., Ramakrishnan, K., and G. Pavlou, "Name-Based Replication Priorities in Disaster Cases", 2nd Workshop on Name Oriented Mobility (NOM), 2014, .

[Seedorf2014]
Seedorf, J., Kutscher, D., 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, .

Appendix A. Acknowledgment

The authors would like to thank Ioannis Psaras for useful comments.

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

Jan Seedorf
NEC
Kurfuerstenanlage 36
Heidelberg 69115
Germany

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

Mayutan Arumaithurai
University of Goettingen
Goldschmidt Str. 7
Goettingen 37077
Germany

Phone: +49 551 39 172046
Fax: +49 551 39 14416
Email: arumaithurai@informatik.uni-goettingen.de

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
University of California
Riverside CA
USA

Email: kkramakrishnan@yahoo.com

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

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