ICNRG
Internet-Draft
Intended status: Informational
Expires: August 2, 2020

J. Seedorf
HFT Stuttgart - Univ. of Applied Sciences
M. Arumaithurai
University of Goettingen
A. Tagami
KDDI Research Inc.
K. Ramakrishnan
University of California
N. Blefari Melazzi
University Tor Vergata

January 30, 2020

Research Directions for Using ICN in Disaster Scenarios
draft-irtf-icnrg-disaster-10

Abstract

Information Centric Networking (ICN) 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 with respect to applying ICN approaches for coping with natural or human-generated, large-scale disasters. This document is a product of the Information-Centric Networking Research Group (ICNRG).

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 https://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 August 2, 2020.

Copyright Notice

Table of Contents

1. Introduction

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

There are existing research and standardization approaches (for instance, see further the work and discussions in the concluded IRTF DTN Research Group [dtnrg] and in the IETF DTN Working Group [dtnwg]) and an IRTF stream Experimental RFC [RFC5050] for Delay/Disruption Tolerant Networking (DTN), which is a key necessity for communicating in the disaster scenarios we are considering in this document (see further Section 3.1). 'Disconnection tolerance' can thus be achieved with these existing DTN approaches. However, while these approaches can provide independence from an existing communication infrastructure (which indeed may not work anymore after a disaster

has happened), ICN offers as key concepts suitable naming schemes and multicast communication which together enable many key (publish/subscribe-based) use cases for communication after a disaster (e.g. message prioritisation, one-to-many delivery of important messages, or group communication among rescue teams, see further Section 4). One could add such features to existing DTN protocols and solutions; however, in this document we explore the use of ICN as starting point for building a communication architecture that supports (somewhat limited) communication capabilities after a disaster. We discuss the relationship between the ICN approaches (for enabling communication after a disaster) discussed in this document with existing work from the DTN community in more depth in Section 3.3 .

'Emergency Support and Disaster Recovery' is also listed among the ICN Baseline Scenarios in [RFC7476] as a potential scenario that 'can be used as a base for the evaluation of different information-centric networking (ICN) approaches so that they can be tested and compared against each other while showcasing their own advantages' [RFC7476] . In this regard, this document complements [RFC7476] by investigating the use of ICN approaches for 'Emergency Support and Disaster Recovery' in depth and discussing the relationship to existing work in the DTN community.

This document focuses on ICN-based approaches that can enable communication after a disaster. These approaches reside mostly on the networking layer. Other solutions for 'Emergency Support and Disaster Recovery', e.g., on the application layer, may complement the ICN-based networking approaches discussed in this document and expand the solution space for enabling communications among users after a disaster. In fact, addressing the use cases explored in this document would require corresponding applications that would exploit the discussed ICN-benefits on the networking layer for users. However, the discussion of applications or solutions outside of the networking layer are outside the scope of this document.

This document represents the consensus of the Information-Centric Networking Research Group (ICNRG); it is not an IETF product and it does not define a standard. It has been reviewed extensively by the ICN Research Group (RG) members active in the specific areas of work covered by the document.

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.

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 to disasters. Mobile phones have become the lifelines for communication including safety confirmation: Besides (emergency) phone calls, services in mobile networks commonly being used after a disaster include network disaster SMS notifications (or SMS 'Cell Broadcast' [cellbroadcast]), available in most cellular networks. 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 and 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 to a small extent predictable using weather forecasting technologies, may have a slower onset, and occur in known geographical regions and seasons, terrorist attacks almost always 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 capabilities 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:

- 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, content integrity, and trust: In mobile networks, users are authenticated via central entities. While special services important in a disaster scenario exist and may work without authentication (such as SMS 'Cell Broadcast' [cellbroadcast] or emergency calls), user-to-user (or user-to-authorities) communication is normally not possible without being authenticated via a central entity in the network. In order to communicate in fragmented or disconnected parts of a mobile network, the challenge of decentralising user authentication arises. Independently of the network being fixed or mobile, data origin authentication and verifying the correctness of content retrieved from the network may be challenging when being 'offline' (e.g., potentially disconnected from content publishers as well as from servers of a security infrastructure which can provide

missing certificates in a certificate chain or up-to-date information on revoked keys/certificates). As the network suddenly becomes fragmented or partitioned, trust models may shift accordingly to the change in authentication infrastructure being used (e.g., one may switch from a PKI to a web-of-trust model such as PGP). Note that blockchain-based approaches are in most cases likely not suitable for the disaster scenarios considered in this document, as the communication capabilities needed to find consensus for a new block as well as for retrieving blocks at nodes presumably will not be available (or too excessive for the remaining infrastructure) after a disaster.

- Delivering/obtaining information and traffic prioritization 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) with higher priority than other content.

- Delay/Disruption Tolerant Approach: Fragmented networks make it difficult to support direct end-to-end communication with small or no delay. However, communication in general and especially during a disaster can often tolerate some form of delay. E.g., in order to know if someone's relatives are safe or not, a corresponding emergency message need not necessarily be supported in an end-to-end manner, but would also be helpful to the human recipient if it can be tranported in a hop-by-hop fashion with some delay. For these kinds of use-cases, it is sufficient to improve communication resilience in order to deliver such important messages.

- 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.

- Contextuality: Like any communication in general, disaster scenarios are inherently contextual. Aspects of geography, the people affected, the rescue communities involved, the languages being used and many other contextual aspects are highly relevant for an efficient realization of any rescue effort and, with it, the realization of the required communication.

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 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.

- Integrity and 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, object integrity of data retrieved from the network can be verified without relying on a trusted third party or PKI. In addition, given that the correct object name is known, such schemes can also provide data origin authentication (see for instance Section 8.3. in [RFC6920])

- Content-based access control: ICN promotes a data-centric communication model which naturally supports content-based security (e.g. allowing access to content only to a specific user or class of users) as in ICN - if desired - not the communication channel is secured (encrypted) but the content itself. This functionality could facilitate trusted communications among peer users in isolated areas of the network where a direct communication channel may not always or continuously exist.

- 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).

- Sessionless: ICN does not require full end-to-end connectivity. This feature facilitates a seemless aggregation between a normal

network and a fragmented network, which needs DTN-like message forwarding.

- Potential to run traditional IP-based services (IP-over-ICN): While ICN and DTN promote the development of novel applications that fully utilize the new capabilities of the ICN/DTN network, work in [Trossen2015] has shown that an ICN-enabled network can transport IP-based services, either directly at IP or even at HTTP level. With this, IP- and ICN/DTN-based services can coexist, providing the necessary support of legacy applications to affected users, while reaping any benefits from the native support for ICN in future applications.

- Opportunities for traffic engineering and traffic prioritization: ICN provides the possibility to perform traffic engineering based on the name of desired content. This enables priority based replication depending on the scope of a given message [Psaras2014] . In addition, as [Trossen2015] , among others, have pointed out, the realization of ICN services and particularly of IP-based services on top of ICN provide further traffic engineering opportunities. The latter not only relate to the utilization of cached content, as outlined before, but to the ability to flexbily adapt to route changes (important in unreliable infrastructure such as in disaster scenarios), mobility support without anchor points (again, important when parts of the infrastructure are likely to fail) and the inherent support for multicast and multihoming delivery.

3.3. ICN as Starting Point vs. Existing DTN Solutions

There has been quite some work in the DTN (Delay Tolerant Networking) community on disaster communication (for instance, see further the work and discussions in the concluded IRTF DTN Research Group [dtnrg] and in the IETF DTN Working Group [dtnwg]). However, most DTN work lacks important features such as publish/subscribe (pub/sub) capabilities, caching, multicast delivery, and message prioritisation based on content types, which are needed in the disaster scenarios we consider. One could add such features to existing DTN protocols and solutions, and indeed individual proposals for adding such features to DTN protocols have been made (e.g. [Greifenberg2008] [Yoneki2007] propose the use of a pub/sub-based multicast distribution infrastructure for DTN-based opportunistic networking environments).

However, arguably ICN---having these intrinsic properties (as also outlined above)---makes a better starting point for building a communication architecture that works well before and after a disaster. For a disaster-enhanced ICN system this would imply the following advantages: a) ICN data mules would have built-in caches

and can thus return content for interests straight on, b) requests do not necessarily need to be routed to a source (as with existing DTN protocols), instead any data mule or end-user can in principle respond to an interest, c) built-in multi-cast delivery implies energy-efficient large-scale spreading of important information which is crucial in disaster scenarios, and d) pub/sub extension for popular ICN implementations exist [COPSS2011] which are very suitable for efficient group communication in disasters and provide better reliability, timeliness and scalability as compared to existing pub/sub approaches in DTN [Greifenberg2008] [Yoneki2007] .

Finally, most DTN routing algorithms have been solely designed for particular DTN scenarios. By extending ICN approaches for DTN-like scenarios, one ensures that a solution works in regular (i.e. well-connected) settings just as well (which can be important in reality, where a routing algorithm should work before and after a disaster). It is thus reasonable to start with existing ICN approaches and extend them with the necessary features needed in disaster scenarios. In any case, solutions for disaster scenarios need a combination of ICN-features and DTN-capabilities.

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.

- 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 a 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, c) source authentication and content integrity so that users can confirm that the messages they receive are indeed from their relatives or friends and have not been tampered with, and d) the support for contextual caching in order to provide the right information to the right set of affected people in the most efficient manner.

- 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) source authentication and content integrity, such that citizens can confirm the correctness and 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. In [Robitzsch2015] , a more elaborate set of requirements is provided that addresses, among disaster scenarios, a communication infrastructure for communities facing several geographic, economic and political challenges.

5. ICN-based Research Approaches and Open Research Challenges

This section outlines some ICN-based research approaches that aim at fulfilling the previously mentioned use cases and requirements (Section 5.1). Most of these works provide proof-of-concept type soluions, addressing singular challenges. Thus, several open issues remain which are summarized in Section 5.2.

5.1. Suggested ICN-based Research Approaches

The research community has investigated ICN-based solutions to address the aforementioned challenges in disaster scenarios. Overall, the focus is on delivery of messages and not real-time communication. While most probably users would like to conduct real-time voice/video calls after a disaster, in the extreme scenario we consider (with users being scattered over different fragmented networks, see Section 2), somewhat delayed message delivery appears to be inevitable, and full-duplex real-time communication seems infeasible to achieve (unless users are in close proximity). Thus, the assumption is that - for a certain amount of time at least (i.e. the initial period until the regular communication infrastructure has been repaired) - users would need to live with message delivery and publish/subscribe services but without real-time communication. Note, however, that a) in principle ICN can support VoIP calls; thus,

if users are in close proximity, (duplex) voice communication via ICN is possible [Gusev2015], and b) delayed message delivery can very well include (recorded) voice messages.

- ICN 'data mules': To facilitate the exchange of messages between different network fragments, mobile entitites 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). An example of a many-to-many communication service for fragmented networks based on ICN data mules has been proposed in [Tagami2016].

- Priority-dependent or popularity-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' decribed in Section 4. In [Seedorf2016], a scheme is presented that enables to estimate the popularity of ICN interest messages in a completely decentralized manner among data mules in a scenario with random, unpredictable movements of ICN data mules. The approach exploits the use of nonces associated with end user requests, common in most ICN architectures. It enables for a given ICN data mule to estimate the overall popularity (among end-users) of a given ICN interest message. This enables data mules to optimize content dissemination with limited caching capabilities by prioritizing interests based on their popularity.

- Information Resilience through Decentralised Forwarding: In a dynamic or disruptive environment, such as the aftermath of a disaster, both users and content servers may dynamically join and leave the network (due to mobility or network fragmentation). Thus, users might attach to the network and request content when the network is fragmented and the corresponding content origin is not reachable. In order to increase information resilience,

content cached both in in-network caches and in end-user devices should be exploited. A concrete approach for the exploitation of content cached in user devices is presented in [Sourlas2015] . The proposal in [Sourlas2015] includes enhancements to the NDN router design, as well as an alternative Interest forwarding scheme which enables users to retrieve cached content when the network is fragmented and the content origin is not reachable. Evaluations show that this approach is a valid tool for the retrieval of cached content in disruptive cases and can be applied to tackle the challenges presented in Section 3.1 .

- 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] .

- 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 calls 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. These schemes enable the source to specify the set of nodes allowed to later on decrypt the content during the encryption process.

- 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.

5.2. Open Research Challenges

The proposed solutions in Section 5.1 investigate how ICN approaches can in principal address some of the outlined challenges. However, several research challenges remain open and still need to be addressed. The following (incomplete) list summarizes some unanswered research questions and items that are being investigated by researchers:

- Evaluation of the proposed mechanisms (and their scalability) in realistic large-scale testbeds with actual, mature implementations (compared to simulations or emulations)

- Specifying for each mechanism suggested to what exact extent ICN deployment in the network and at user equipment is required or would be necessary, before and after a disaster.

- 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?

- Build and test real (i.e. not early-stage prototypes) ICN data mules by means of implementation and integration with lower layer hardware; conduct evaluations of decentralised forwarding schemes in real environments with these actual ICN data mules

- How to derive concrete policies for ICN-style name-based prioritized spreading of information?

- Further investigate, develop, and verify mechanisms that address energy efficiency requirements for communication after a disaster

- 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?

6. Security Considerations

This document does not define a new protocol (or protocol extension) or a particular mechanism, and therefore introduces no specific new security considerations. General security considerations for Information-Centric Networking -- which also apply when using ICN networking techniques to communicate after a disaster -- are discussed in [RFC7945].

The after-disaster communication scenario which is the focus of this document raises particular attention to decentralised authentication, content integrity, and trust as key research challenges (as outlined in Section 3.1). The corresponding use cases and ICN-based research approaches discussed in this document thus imply certain security requirements. In particular data origin authentication, data integrity, and access control are key requirements for many use cases in the aftermath of a disaster (see Section 4).

In principle, the kinds of disasters discussed in this document can happen as a result of a natural disaster, accident or by human-error. However, also intentional actions can cause such a disaster (e.g., a terrorist attack, as mentioned in Section 2). In this case, i.e., intentionally caused disasters by attackers, special attention needs to be paid when re-enabling communications as temporary, somewhat un-reliable communications with potential limited security features may be anticipated and abused by attackers (e.g., to circulate false messages to cause further intentional chaos among the human population, to leverage this less secure infrastructure to refine targeting, or to track the responses of security/police forces). Potential solutions on how to cope with intentionally caused disasters by attackers and on how to enable a secure communications

infrastructure after such an intentionally caused disaster are out of scope of this document.

The use of data-centric security schemes such as 'Ciphertext-Policy Attribute Based Encryption' (as mentioned in Section 5.1) which encrypt the data itself (and not the communication channel), in principle allows for the transmission of such encrypted data over an unsecured channel. However, still metadata about the encrypted data being retrieved arises. Such metadata may disclose sensitive information to a network-based attacker even if such an attacker cannot decrypt the content itself.

This document has summarized research directions for addressing these challenges and requirements, such as efforts in data-centric confidentiality and access control as well as recent works for decentralised authentication of messages in a disaster-struck networking infrastructure with non-functional routing links and limited communication capabilities (see Section 5).

7. Conclusion

This document has outlined 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 has described high-level research challenges for enabling communication after a disaster has happened as well as a general rationale why ICN approaches could be beneficial to address these challenges. Further, concrete use cases have been described and how these can be addressed with ICN-based approaches has been discussed.

Finally, the document provided an overview of examples of existing ICN-based solutions that address the previously outlined research challenges. These concrete solutions demonstrate that indeed the communication challenges in the aftermath of a disaster can be addressed with techniques that have ICN paradigms at their base, validating our overall reasoning. However, further, more detailed challenges exist and more research is necessary in all areas discussed: efficient content distribution and routing in fragmented networks, traffic prioritization, security, and energy-efficiency. An incomplete, high-level list of such open research challenges has concluded the document.

In order to deploy ICN-based solutions for disaster-aftermath communication in actual mobile networks, standardized ICN baseline protocols are a must: It is unlikely to expect all user equipment in a large-scale mobile network to be from the same vendor. In this respect, the work being done in the IRTF ICNRG is very useful as it works towards standards for concrete ICN protocols that enable

interopability among solutions from different vendors. These protocols - currently being standardized as IRTF stream Experimental specifications in the IRTF INCRG - provide a good foundation for deploying ICN-based disaster-aftermath communication and thereby addressing key use cases that arise in such situations (as outlined in this document).

8. IANA Considerations

This document requests no IANA actions.

9. References

9.1. Normative References

[RFC5050] Scott, K. and S. Burleigh, "Bundle Protocol Specification", RFC 5050, DOI 10.17487/RFC5050, November 2007, <https://www.rfc-editor.org/info/rfc5050>.

[RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, DOI 10.17487/RFC6920, April 2013, <https://www.rfc-editor.org/info/rfc6920>.

[RFC7476] Pentikousis, K., Ed., Ohlman, B., Corujo, D., Boggia, G., Tyson, G., Davies, E., Molinaro, A., and S. Eum, "Information-Centric Networking: Baseline Scenarios", RFC 7476, DOI 10.17487/RFC7476, March 2015, <https://www.rfc-editor.org/info/rfc7476>.

[RFC7945] Pentikousis, K., Ed., Ohlman, B., Davies, E., Spirou, S., and G. Boggia, "Information-Centric Networking: Evaluation and Security Considerations", RFC 7945, DOI 10.17487/RFC7945, September 2016, <https://www.rfc-editor.org/info/rfc7945>.

9.2. Informative References

[cellbroadcast] Wikipedia, "Cell Broadcast - Wikipedia, https://en.wikipedia.org/wiki/Cell_Broadcast", (online).

[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.

[dtnrg] Fall, K. and J. Ott, "Delay-Tolerant Networking Research Group - DTNRG", https://irtf.org/dtnrg.

[dtnwg] Fall, K. and J. Ott, "Delay/Disruption Tolerant Networking WG", https://tools.ietf.org/wg/dtn/.

[Greifenberg2008] Greifenberg, J. and D. Kutscher, "Efficient publish/subscribe-based multicast for opportunistic networking with self-organized resource utilization", Advanced Information Networking and Applications-Workshops, 2008.

[Gusev2015] Gusev, P. and J. Burke, "NDN-RTC: Real-Time Videoconferencing over Named Data Networking", 2nd ACM Conference on Information-Centric Networking (ICN 2015), Sep. 30 - Oct. 2, San Francisco, CA, USA.

[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.

[Robitzsch2015] Robitzsch, S., Trossen, D., Theodorou, C., Barker, T., and A. Sathiaseel, "D2.1: Usage Scenarios and Requirements"", H2020 project RIFE, public deliverable, 2015.

[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.

[Seedorf2016] Seedorf, J., Kutscher, D., and B. Gill, "Decentralised Interest Counter Aggregation for ICN in Disaster Scenarios", Workshop on Information Centric Networking Solutions for Real World Applications (ICNSRA), 2016.

[Sourlas2015] Sourlas, V., Tassiulas, L., Psaras, I., and G. Pavlou, "Information Resilience through User-Assisted Caching in Disruptive Content-Centric Networks", 14th IFIP NETWORKING, May 2015.

[Tagami2016]
Tagami, A., Yagyu, T., Sugiyama, K., Arumaithurai, M., Nakamura, K., Hasegawa, T., Asami, T., and K. Ramakrishnan, "Name-based Push/Pull Message Dissemination for Disaster Message Board", The 22nd IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), 2016.

[Trossen2015]
Trossen, D., "IP over ICN - The better IP?", 2015 European Conference onNetworks and Communications (EuCNC), June/July 2015, pp. 413 - 417.

[Yoneki2007]
Yoneki, E., Hui, P., Chan, S., and J. Crowcroft, "A socio-aware overlay for publish/subscribe communication in delay tolerant networks", Proceedings of the 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems, 2007.

Appendix A. Acknowledgment

The authors would like to thank Ioannis Psaras for useful comments. Also, the authors are grateful to Christopher Wood and Daniel Corujo for valuable feedback and suggestions on concrete text for improving the document. Further, the authors would like to thank Joerg Ott and Dirk Trossen for valuable comments and input, in particular regarding existing work from the DTN community which is highly related to the ICN approaches suggested in this document. Also, Akbar Rahman provided useful comments and usggestions, in particular regarding existing disaster warning mechanisms in today's mobile phone networks.

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. More information is available at the project web site http://www.greenicn.org/.

Authors' Addresses

Jan Seedorf
HFT Stuttgart - Univ. of Applied Sciences
Schellingstrasse 24
Stuttgart 70174
Germany

Phone: +49 711 8926 2801
Fax: +49 711 8926 2553
Email: jan.seedorf@hft-stuttgart.de

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 Research Inc.
2-1-15 Ohara
Fujimino, Saitama 356-85025
Japan

Phone: +81 49 278 73651
Fax: +81 49 278 7510
Email: tagami@kddi-research.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