Disciplines and Measures of Information Resilience

Jacek Rak[1], Magnus Jonsson[2], David Hutchison[3], James P.G. Sterbenz[3,4,5]

[1]*Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics, PL*
[2]*Halmstad University, Centre for Research on Embedded Systems (CERES), SE*
[3]*Lancaster University, School of Computing and Communications, UK*
[4]*The University of Kansas, EECS and Information and Telecommunication Technology Center, USA*
[5]*The Hong Kong Polytechnic University, Kowloon, Hong Kong*

e-mail: [1]jrak@pg.edu.pl, [2]magnus.jonsson@hh.se, [3]d.hutchison@lancaster.ac.uk, [4]jpgs@ittc.ku.edu

ABSTRACT

Communication networks have become a fundamental part of many critical infrastructures, playing an important role in information delivery in various failure scenarios triggered e.g., by forces of nature (including earthquakes, tornados, fires, etc.), technology-related disasters (for instance due to power blackout), or malicious human activities. A number of recovery schemes have been defined in the context of network resilience (with the primary focus on communication possibility in failure scenarios including access to a particular host, or information exchange between a certain pair of end nodes). However, because end-users are becoming more and more interested in information itself (regardless of its physical location in the network), it is appropriate to complement the well-defined framework of network resilience with one that addresses information resilience, and to introduce definitions of relevant disciplines and measures, as proposed in this paper.

Keywords: information resilience, survivability, disruption tolerance, dependability; communication networks, information-centric networking, metrics, failures

1. Introduction

Due to the convergence of telecommunications, media, and information technology accompanied by a rapid growth of traffic volume carried across communication networks, a transition of communication interest can be observed from host-based towards information-based [1]-[2]. Indeed, users now simply look for information (rather than for access to a particular host) regardless of its physical location. In the literature such a concept, in which the task to determine the location of information and deliver it to the user is left to the network, is referred to as **information-centric networking** (**ICN**), or **content-centric networking** (**CCN**) [1], [2]. ICN architectures commonly make use of **anycasting** – a transmission scheme able to deliver information to a requesting unit from one out of many possible locations – and **pub/sub** (publish/subscribe) message/information exchange [1], [2].

As the performance of communication networks frequently suffers from a number of disruptive events, various techniques based on utilization of alternate communication paths have been introduced to maintain the possibility of transmission in the case of failures of single or multiple network nodes and links. These backup paths can be either established dynamically after a failure (known as the reactive restoration approach [2]) or set up in advance (referred to as the pre-planned protection scheme [2]). The objective of these mechanisms is to assure the **network resilience** defined in [3] as *the ability of a network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation*.

A detailed classification of network resilience disciplines expanding beyond dependability on those introduced by Avizienis et al. in [4] is presented in [3] by Sterbenz et al. As shown in Fig. 1, it includes six major disciplines, namely: **survivability**, **traffic tolerance**, **disruption tolerance**, **dependability**, **security** and **performability**. However, this classification was originally introduced primarily for the network resilience context. As there is currently no classification available in the literature aimed to define the related disciplines and measures of **information resilience**, the aim of this paper is to fill the gap by proposing a refinement of the original classification from [3] to adapt it to the context of information-centric networking.

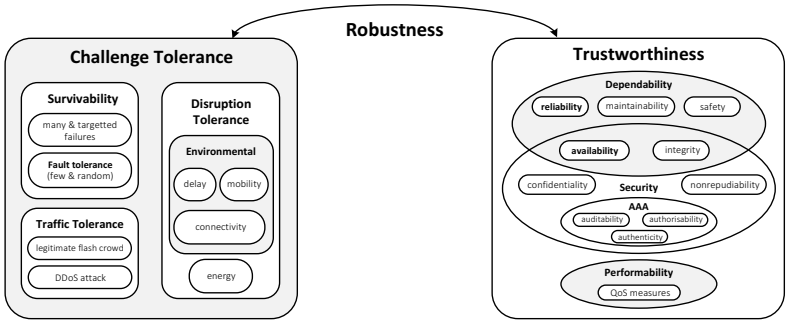

Fig. 1 Classification of network resilience disciplines from [3].

In the remainder of this paper, a definition of information resilience is first introduced in Section 2 and is followed by a discussion on its relation to the network resilience paradigm. Section 3, in turn, proposes definitions of relevant disciplines and measures of information resilience. Section 4 concludes the paper.

2. Information Resilience vs. Network Resilience

The observed shift of end-user communication interest towards information-oriented networking increases the importance of ICN solutions in the context of emerging architectures of communication networks (in particular of the Future Internet). Additionally, the use for example of anycasting enabling retrieval of information from several sources of replicated content can provide a kind of a natural resilience at practically no extra cost. This is also true in the case of failure of a node being the source of information (as shown in Fig. 2), which is not possible for the common unicast transmission. However, some overhead in the context of management is necessary for anycasting to assure the recovery of the affected streams in a timely manner.

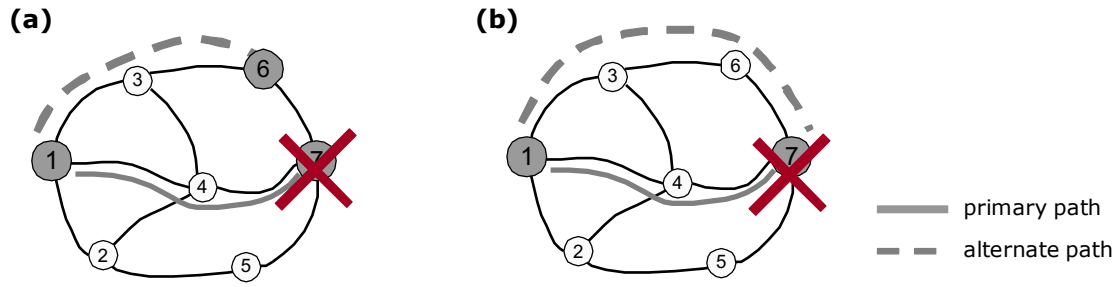

Fig. 2 Example illustrations of: (**a**) anycast communications providing resilience also in the context of a failure of a node hosting the information and (**b**) conventional unicast scheme not able to provide protection against a failure of the end node of a communication path (even if alternate paths are installed).

Any information-related recovery scheme should be also resistant to scenarios of failures of alternate sources of information, so we define **information resilience** as *the ability of a network to provide users with continued access to information in the face of various faults and challenges to normal operation*. Since ICN solutions are meant to coexist with the common network recovery mechanisms applied for host-based communications [1], information resilience is in fact an extension of (not replacing) the network resilience model and mechanisms.

An efficient scheme of information resilience is crucial in the context of disaster scenarios when massive disruptions not only affect the performance of a network (e.g., as a result of multiple correlated failures), but also (and often primarily) have a long-lasting negative impact on the quality of a human life [5]–[7]. A wide range of these events follow from the occurrence of earthquakes, volcanic eruptions, hurricanes, tsunamis, power blackouts, or human-induced failures (including acts of terrorism or other malicious activities aimed to cause maximum degradation of the network performance or to make critical information non-accessible). Particularly in the context of these events, a common expectation is that the global communication infrastructure would still remain operational and allow people to exchange information with relatives and colleagues, as well as to enable receiving of information disseminated from legal authorities to citizens in a timely manner. From the user perspective, information itself is of course one of the most desired assets, regardless of its physical location in the network (as long as its source can be trusted).

The majority of disaster scenarios also imply a significant increase in traffic volume to be transmitted over the communication network (in particular in areas affected by a disaster). At the same time, in the case of network partitions after massive failures, network infrastructure may be only partially available, which in turn implies serious concerns related with information availability [8]. Since post-disaster degradation of a network performance is evident, in the early stage of a network design (and then later during further evolution of the network architecture) it is vital to assure a number of information resilience properties – many of which need definitions and related measures, as proposed in the next section of this paper.

3. Disciplines and Measures of Information Resilience

Similar to the network resilience concept from [3], classification of disciplines in information resilience can be based on challenge tolerance and trustworthiness categories. However, concerning information-oriented communications, we propose to assume that:

- **challenge tolerance** disciplines are related with the network design issues to provide undisturbed access to information in the face of challenges,
- **trustworthiness** disciplines aim to define the measurable characteristics of information resilience.

Robustness, the control theoretic notion to the measurable response of a perturbed system, denoting the relation between challenge tolerance and trustworthiness (see Fig. 1), should be viewed as *an indicator of a network's ability to deliver information successfully when challenged*.

For information resilience, a refinement of definitions of challenge tolerance disciplines is needed as follows:

- **survivability** should be defined as *the ability of a system to deliver relevant information to the user in a timely manner in the presence of challenges resulting in multiple correlated failures, typically in the form of a coordinated attack or large-scale disaster*. The word "mission" from the original definition of survivability from [3] in this context means assuring information availability and delivery to the user,
- **fault tolerance** should mean *the ability of a communication system to provide the user with relevant information in spite of faults resulting from events other than service failures*. As noted in [3], fault tolerance here also does not cover the case of multiple failures,
- **disruption tolerance,** originally denoting the ability of a system to tolerate disconnections of its components (due to weak or intermittent connectivity, mobility, unpredictably long delay, and energy constraints) [3], should now refer to *the ability of a communication system to deliver relevant information to the user despite disconnections or failures of system components and information repositories during and after disruptions*,
- **traffic tolerance** should refer to *the ability of a communication network to serve the increased traffic during and after challenges. This includes increased requests related with information retrieval, as well as any other information exchange such as telepresence and BitTorrent.* Such a definition is justifiable since compared to the traffic tolerance concept given in [3] for the network resilience, information resilience puts a special focus on the ability of a network to accommodate the increased traffic volume as a consequence of legitimate user attempts to retrieve and exchange information (i.e., post-disaster activities of users).

Trustworthiness originally defined in the literature as "the assurance that the communication system will perform as expected" [4] should be redefined for information resilience to denote *the assurance that the communication system will enable the user to access and exchange the relevant information regardless of the failure scenario*. Trustworthiness includes three disciplines, namely: **dependability**, **security,** and **performability**.

In particular, the original definition of **dependability** from [4] should be refined to quantify the service reliance in the context of information accessibility and retrieval. In other words, for information resilience it can be defined as *the ability to deliver or exchange information.*

Measures of dependability are defined in our paper as follows:

- **reliability** (***R***) measuring *the continuity of information accessibility*, being the probability that the information remains accessible for a user regardless of the physical location of information in the network in time frame (0, *t*), as given by: $R(t) = \Pr(\text{information is accessible in } [0, t])$,
- **availability** determining *the readiness of a network to deliver or exchange information*, being the probability that information can be exchanged at a given time,

  The importance of information availability vs. information reliability depends on whether information access is important (such as with an HTTP transaction or CDN push), or an information exchange session is important (as explained in [2]),
- **maintainability,** originally defined as a predisposition of a system to updates (or evolution) measured with respect to downtime [4], should now denote *the ability of a network to maintain information during periods of system updates/evolution*,
- **safety** denotes that the unavailability of information will not lead to catastrophic consequences, in particular severe injury or loss of human or animal life, or catastrophic consequences to the environment,
- **integrity** should define *the assurance that retrieved information has neither been tampered with nor damaged through any activity/system error since the previous authorised access to information.*

We define **information security** as *the ability of a communication system to defend itself from unauthorised access to/update of information*. Following [3], information security can be further characterised in terms of availability and integrity (also characterising dependability), as well as concerning its own properties listed in [3] refined in this paper in the context of information resilience as follows:

- **confidentiality** is *the assurance that regardless of the failure scenario, information is made available only to authorised individuals*,
- **non-repudiability** is *the possibility to guarantee the integrity and availability of the identity of a sender/receiver of the information regardless of the failure scenario*,
- **auditability** is *the information security assessment possible regardless of the failure scenario*,
- **authorisability** is *an approval granted to an entity (system/user) to access information*,
- **authenticity** is *the confirmed truthfulness of a piece of information claimed true by an entity*.

Performability was originally defined as the level of performance defined in terms of QoS measures including delay, jitter, throughput/goodput and packet delivery ratio [4]; with respect to dependability, performability considers *degraded performance* of a complex system rather than a component being operational or failed. In the context of information resilience, performability can be specified *as the ability of a network to deliver the required QoS performance in the context of information exchange regardless of the failure scenario.* As network performance under massive failures will be reduced, it is hardly possible that QoS characteristics could be kept unchanged. Therefore, for any failure scenario it is reasonable to expect that performability will be either **full** or **degraded** (compared with the expected QoS performance in a normal operational state).

4. Conclusion

The observed shift of user activities in communication networks towards information exchange has motivated network operators to apply architecture focused on content delivery and replication, including caches and CDNs. Because the need to exchange relevant and up-to-date information is naturally magnified in scenarios of massive failures, it is important not only to deploy the respective mechanisms to improve the performance of communication networks under disruptions, but also to be able to measure the performance of a network in terms of information accessibility and delivery. To fill in the gap related with missing disciplines and measures of information resilience in the literature, in this paper we have proposed the refinement of the original classification from [3] by adapting it to the context of information-centric networking.

5. Acknowledgement

This article is based on work in COST Action CA15127 ("Resilient communication services protecting end-user applications from disaster-based failures – RECODIS") supported by COST (European Cooperation in Science and Technology). The work of Jacek Rak was also partially supported by the Statutory Fund of the Faculty of Electronics, Telecommunications and Informatics of Gdansk University of Technology, Poland.

References

[1] M.F. Al-Naday, M.J. Reed, D. Trossen, K. Yang: Information resilience: source recovery in an information-centric network. IEEE Network, vol. 28, no. 3, pp. 36-42 (2014)

[2] J. Rak: *Resilient routing in communication networks*, Springer (2015)

[3] J.P.G. Sterbenz, D. Hutchison, E.K. Çetinkaya, A. Jabbar, J.P. Rohrer, M. Schöller, P. Smith: Resilience and survivability in communication networks: strategies, principles, and survey of disciplines. Computer Networks, Elsevier, vol. 54, no. 8, pp.1245-1265 (2010)

[4] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr: Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33 (2004)

[5] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, L. Wosinska: RECODIS: resilient communication services protecting end-user applications from disaster-based failures. Proc. ICTON 2016 (18th International Conference on Transparent Optical Networks), pp. 1-4 (2016)

[6] A. Mauthe, D. Hutchison, E.K. Çetinkaya, I. Ganchev, J. Rak, J.P.G. Sterbenz, M. Gunkel, P. Smith, T. Gomes: Disaster-resilient communication networks: principles and best practices. Proc. RNDM 2016 (8th International Workshop on Resilient Networks Design and Modeling), pp. 1-10 (2016)

[7] Webpage of CA15127-RECODIS Action: *http://www.cost-recodis.eu*

[8] V. Sourlas, L. Tassiulas, I. Psaras, G. Pavlou: Information resilience through user-assisted caching in disruptive content-centric networks. Proc. Networking 2015 (IFIP Networking Conference), pp. 1-5 (2015)