Report of Short Term Scientific Mission of COST CA15127-RECODIS

STSM Topic: **Taxonomy of Disciplines and Measures of Information Resilience under Disaster-based Disruptions**

STSM Applicant: Jacek Rak (MC Chair), Gdansk University of Technology, Poland
Host: Magnus Jonsson (MC Member), Halmstad University, Sweden

Period: January 15-20, 2017
Working Group: WG5

1. Purpose of the STSM

Communication networks have become an important part of the critical information infrastructure. They have shown to play a crucial role especially in case of disaster scenarios (e.g., earthquakes, tornados, fires, etc.) of an undeniably negative impact on humans on a massive scale. Post-disaster degradation of communication networks performance often lasting for a long time is evident, and is additionally enforced by the increased network load due to activities of people desperately trying to communicate with each other, or repeatedly requesting the up-to-date-information.

Communication networks resilience defined in "Resilience and survivability in communication networks: strategies, principles, and survey of disciplines" (2010) 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, helps us to maintain/restore the transmission possibility. It has been well defined in the literature before. However, since information has undoubtedly become the most desired property (especially in disaster scenarios), people are becoming more and more interested in access to particular information/content rather than simply in getting access to the network/particular server. This in turn raises the need to provide the respective definitions and measures to make a proper shift towards the information resilience concept, which has not been defined so far (particularly under disaster-based disruptions).

The objective of this STSM is thus to work out the definitions of information resilience along with its respective disciplines and measures with a special focus on disaster-based failures. This is necessary to form a common basis for any further activity in the framework of CA15127-RECODIS focused on assuring information resilience in disaster scenarios. One of possible methods to achieve this objective is to provide a refinement of the respective state-of-the-art definitions of communications resilience.

2. Description of Results

Information has undoubtedly become one of the most desired properties. Instant access to information is commonly demanded nowadays at any time and location. This need is especially magnified in case of a number of disaster scenarios when large regions suffer from the negative effects of disasters. Example scenarios cover e.g., earthquakes, volcano eruptions, hurricanes, or heavy rain falls. All these cases make people try to (desperately) communicate with each other, implying a rapid increase of a number of demands given to communication network already suffering from physical failures of its elements.

In particular, disasters bring about massive failures of network elements located in a given area, referred to as a *region failure*. It is worth noting that performance of a communication network can be degraded not only as a result of weather-based factors. We should mention here a number of technology-related massive disruptions (e.g., power blackouts related with unavoidable interdependence between communication networks and power grids), or malicious human activities in the form of attacks aimed to cause as much degradation of communication network performance as possible.

We have been also observing a change of primary objective of a communication network (originally to provide the end-to-end connectivity) towards content connectivity. It means that unlike in the past, users are becoming more and more interested in getting access to information (regardless of its physical location) rather than in the ability to proceed with end-to-end transmission between specified end nodes (or getting access to a particular network / server). This in turn raises the need to refine the common definitions and measures related with resilience of communication networks, as presented e.g., in [Ster10] to adapt them to the *information resilience* context. This issue has not been covered in the literature so far also in the aspect of resilience under disaster-based disruptions.

2a. Communication Networks Resilience – Common Disciplines and Measures

The most comprehensive survey proposed so far for resilience disciplines and measures seems to be the one by Sterbenz *et al.* from [Sterb10]. Other classifications are available e.g., in [Lap94], [Lap05], or [Mar14].

Network resilience is defined in [Sterb10] 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". Following [Ster10], resilience disciplines include two following main categories shown in Fig. 1.

- *challenge tolerance* comprising approaches of network design aimed to provide service continuity in the face of challenges,
- *trustworthiness* referring to measurable characteristics of communication systems.

Robustness (defining the relation between challenge tolerance and trustworthiness), is in turn the viewed as an indicator of network performance under perturbative conditions.

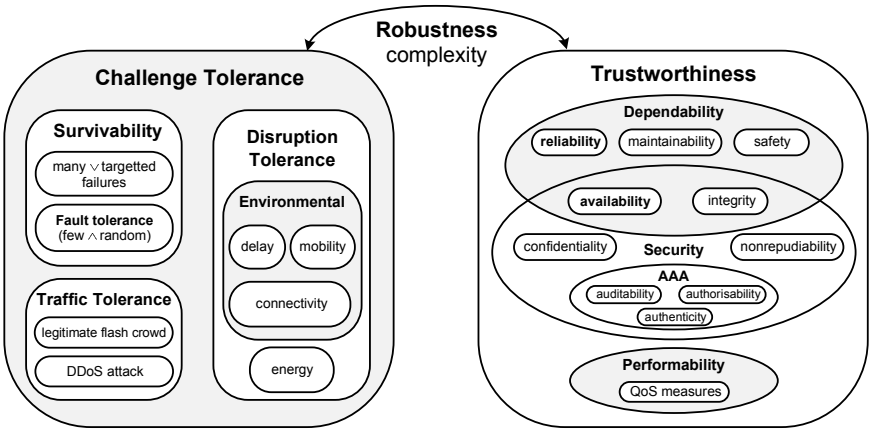

Fig. 1 Classification of resilience disciplines and measures from [Sterb10].

[Sterb10] provides a further decomposition of challenge tolerance into:

- *survivability* referring to communication networks infrastructure, which is defined as the capability of a system to fulfil its mission in a timely manner, in the presence of threats including attacks or natural disasters (please see e.g., [Haid04] for another definition of survivability viewed as the ability of a network to recover the affected traffic in failure environments and to provide different services continuously, [Kia09] where it is defined as the ability of a network to continue the service in the presence of failures, or [Chol10] extending the survivability definition to cover both physical and software faults),
- *fault tolerance* is viewed as the ability of a communication system to cope with faults being result of events other than service failures. However, as fault tolerance is not sufficient to provide recovery after multiple failures, and therefore, it is considered in [Ster10] as a subset of survivability only[1]

[1] As given in [Sterb10], survivability has a broader meaning than fault tolerance in a sense that it also comprises issues of correlated failures occurring for instance due to malicious human activities [Cucu12], or failures of a subset of network elements located in a given area [Agar11] (also in the context of unbounded networks) [Muk14]. It is important to notice that apart from redundancy (implying

- *disruption tolerance* denotes resistance of communication paths to disruptions. Indeed, following [Ster10], it can be defined as the ability of a system to tolerate disruptions in connectivity among its components (evaluated with respect to characteristics of communication paths [Khab12] subject to a number of issues including e.g., a dynamic behaviour of a network (for instance in VANETs [Sich08]), delays that are not tolerated by traditional network protocols (see satellite communication issues in [Cai11]), or energy constraints related with the operational time of nodes (as in Wireless Sensor Networks [Ming13]).
- *traffic tolerance* being the ability of a network to accommodate increased traffic volumes. Indeed, traffic can be a challenge, if its volume raises far beyond the general network design assumptions, as e.g., in case of flash crowd following e.g., from malicious actions including DDoS attacks [Geva14].

Trustworthiness is defined in the literature as the assurance that the communication system will perform as expected [Aviz04]. It provides a general set of measures of service delivery and includes three disciplines, namely: dependability, security, and performability.

Dependability is defined as a discipline introduced to quantify the level of service reliance. It provides five following measures:

- *reliability* (*R*) used to measure the level of service continuity being the probability that a system/service remains operable in time frame (0, *t*), as given by formula (1).

$$R(t) = \Pr(\text{no failure in } [0, t]) \quad (\mathbf{1})$$

- *availability* (*A*) viewed as the readiness of a communication system for its usage at time *t* as defined by formula (2)

$$A(t) = \sum_{i \in W} P_i(t) \quad (\mathbf{2})$$

where:

W is the set of states in which the system is operating correctly,

$P_i(t)$ is the probability that a system is in state *i* at time *t*.

In practice, it is commonly estimated by the availability indicator given by formula (3).

$$A = \frac{MTTF}{MTBF} = \frac{MTTF}{MTTF + MTTR} \quad (\mathbf{3})$$

where:

MTTF is the mean time to failure (i.e., the length of a time period during which the service is not interrupted),

MTBF is the mean time between consecutive failures,

MTTR is the mean time to repair.

Reliability is suitable for session/connection-oriented applications (for which MTTF should be relatively long), while availability better works for transactional services with short-time operations (e.g., HTTP) only requiring MTTR to be relatively short.

- *maintainability* defined as a predisposition of a system to updates (or evolution),
- *safety* used to measure the level of a system dependability under catastrophic failures. It refers to the effect rather than the cause of a failure.

---

allocation of additional network resources to provide backup solutions), survivability additionally requires diversity to guarantee that a given failure scenario does not affect multiple mechanisms of a communication system at the same time (e.g., both a primary and a backup path of a demand) [Miss13], [Rak15] under multiple (and correlated) failures.

- *integrity* being a measure of the absence of unauthorized (improper) system modifications.

Security is in turn defined as the ability of a communication system to defend itself from unauthorized activities of third parties. As given in Fig. 1, security has several joint properties with dependability (i.e., *availability* and *integrity*). Individual measures of security in turn include [Land01]:

- *authenticity* - assurance that a given principal is who he/she claims to be,
- *authorisability* - assurance assuring that a given originator / creator of information principal is who he/she claims to be,
- *auditability* - a measure of degree to which extent the events can be traced (from originator of the event, its approver, and final disposition),
- *confidentiality* - assurance that any information is not disclosed without a proper authorization,
- *non-repudiability* - assurance that any neutral third party (neutral) can be convinced that a particular event did (or did not) occur.

Performability provides measures of system performance related with QoS requirements (defined in terms of delay, jitter, throughput/goodput, and packet delivery ratio).

2b. Information Resilience – Proposed Taxonomy of Disciplines and Measures

Contrary to communication networks resilience, in case of information it is crucial to focus not only on availability of a communication path between a certain pair of end nodes, but on making information accessible regardless of the failure scenario. This is reasonable, since for users, it is commonly sufficient to get information from whichever location storing its copy (assuming that the copy was verified to be not a fake). This can be provided e.g., via anycast mechanisms. Therefore, in terms of access to information, resilience disciplines need to be developed, and the most straightforward way to do this seems to be by refinement of the respective definitions of communications resilience to adapt them to the context of information resilience.

Information resilience can be defined as *the ability of a network to provide users with access to information regardless of its location in the face of various faults and challenges to normal operation*.

Similar to communications resilience, disciplines and measures of information resilience can be categorized into:

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

In the context of information resilience, *robustness* (defining the relation between challenge tolerance and trustworthiness) should be viewed as an indicator of network performance to provide access to information under perturbative conditions.

A set of challenge tolerance disciplines should be adjusted to the context of information resilience as follows:

- *survivability* should be viewed as *the continuous ability of a system to deliver the requested information in a timely manner in the presence of threats including attacks or natural disasters*,
- *fault tolerance* should refer to *the ability of a communication system to provide access to information in case of faults being result of events other than service failures* (not necessarily covering the cases of multiple failures),
- *disruption tolerance* should denote *resistance of a communication system to disruptions allowing for information delivery in such scenarios* (also raising issues of partial connectivity as e.g., in mobile networks or under massive failures),

- *traffic tolerance* in the context of requests to deliver information, should denote *the ability of a network to accommodate the increased number of requests to get information*. Compared to the common traffic tolerance defined for communication systems, here we should focus mainly on increased traffic volumes as a consequence of legitimate attempts to get relevant information by respective valid entities (e.g., as a result of disaster-based failures).

Trustworthiness definition in turn does not need refinement (defined in the literature as the assurance that the communication system will perform as expected [Aviz04]), except for the meaning of the word "perform", which in the context information resilience should be specified as to "deliver information regardless of its location". Since trustworthiness includes three disciplines, namely: dependability, security, and performability, their definitions adapted to the information resilience context (as well as the respective refined measures) are as follows.

Dependability should be now viewed as a discipline aimed to quantify the level of service reliance in the context of information accessibility. Its measures are as follows:

- *reliability* (*R*) measuring the level of continuity of information accessibility being the probability that the information remains accessible in a communication network regardless of its physical location in time frame (0, *t*), as given by formula (1).

$$R(t) = \Pr(\text{information is accessible in } [0, t]) \quad (\mathbf{4})$$

- *availability* (*A*) viewed as the probability that information can be retrieved at time *t* as defined by formula (2)

$$A(t) = \sum_{i \in W} P_i(t) \quad (\mathbf{5})$$

where:

W is the set of states in which a copy of information is accessible from whatever location,

$P_i(t)$ is the probability that a communication system is in state *i* at time *t*.

- *maintainability* originally defined as a predisposition of a system to updates (or evolution), should provide information on how accessible the information is under possible updates of a system,
- *safety* used to measure the level of a system dependability under catastrophic failures. In the context of information resilience it should denote the level of reliance on a system to provide the user with access to demanded information in failure scenarios.
- *integrity* being a measure that retrieved information has neither been tampered/damaged through any activity / system error since the previous authorized access

Security can be defined as *the ability of a communication system to defend itself from unauthorized access to/update of information*.

Performability (in the context of information resilience) provides measures of system performance related with QoS requirements (defined in terms of delay, jitter, throughput/goodput, and packet delivery ratio characterizing retrieval of information).

3 Foreseen joint work / publications resulting from the STSM

STSM Applicant with foresees further co-operation with STSM Host in the context of information resilience, and possible a conference / journal publication.

References

[Agar11] Agarwal, P.K., Efrat, A., Ganjugunte, S., Hay, D., Sankararaman, S., Zussman, G.: The resilience of WDM networks to probabilistic geographical failures. In: Proc. 30th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM'11), 1521-1529 (2011)

[Aviz04] Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. Technical Research Report TR2004-47, Institute for Systems Research, The University of Maryland (2004)

[Cai11] Caini, C., Cruickshank, H., Farrell, S., Marchese, M.: Delay- and disruption-tolerant networking (DTN): an alternative solution for future satellite networking applications. Proceedings of the IEEE. 99(11), 1980-1997 (2011)

[Chol10] Chołda, P., Jajszczyk, A.: Recovery and its quality in multilayer networks. IEEE/OSA Journal of Lightwave Technology. 28(4), 372-389 (2010)

[Cucu12] Cucurull, J., Asplund, M., Nadjm-Tehrani, S., Santoro, T.: Surviving attacks in chal-lenged networks. IEEE Transactions on Dependable and Secure Computing. 9(6), 917 929 (2012)

[Geva14] Geva, M., Herzberg, A., Gev, Y.: Bandwidth Distributed Denial of Service: attacks and defences. IEEE Security & Privacy. 12(1), 54-61 (2014)

[Haid04] Haider, A., Harris, R.: Recovery techniques in Next Generation Networks. IEEE Com-munications Surveys & Tutorials. 9(3), 2-17 (2004)

[Khab12] Khabbaz, M.J., Assi, C.M., Fawaz, W.F.: Disruption-tolerant networking: a comprehen-sive survey on recent developments and persisting challenges. IEEE Communications Surveys & Tutorials. 14(2), 607-640 (2012)

[Kia09] Kiaei, M.S., Assi, C., Jaumard, B.: A survey on the *p*-cycle protection method. IEEE Communications Surveys & Tutorials. 11(3), 53-70 (2009)

[Mar14] Maruyama, H., Legaspi, R., Minami, K., Yamagata, Y.: General resilience: taxonomy and strategies. In: Proc. 2014 International Conference and Utility Exhibition on Green Energy for Sustainable Development (ICUE'14), 1-8 (2014)

[Ming13] Mingsen, X., Wen-Zhan, S., Deukhyoun, H., Jong-Hoon, K., Byeong-Sam, K.: ECPC: preserve downtime data persistence in disruptive sensor networks. In: Proc. IEEE Mobile Ad-Hoc and Sensor Systems (MASS'13), 281-289 (2013)

[Miss13] Misseri, X., Gojmerac, I., Rougier, J.-L.: IDRD: enabling inter-domain route diversity. In: Proc. IEEE International Conference on Communications (IEEE ICC'13), 3536 3541 (2013)

[Muk14] Mukherjee, B., Habib, M.F., Dikbiyik, F.: Network adaptability from disaster disruptions and cascading failures. IEEE Communications Magazine. 52(5), 230-238 (2014)

[Lap05] Laprie, J.-C.: Resilience for the scalability of dependability. In: Proc. Fourth IEEE International Symposium on Network Computing and Applications, 5-6 (2005)

[Lap94] Laprie, J.-C.: Dependability: basic concepts and terminology. IFIP Working Group 10.4 – Dependable Computing and Fault Tolerance (1994)

[Land01] Landwehr, C.E.: Computer Security, International Journal on Information Security, vol. 1, no. 1, pp. 3-13 (2001)

[Rak15] Rak, J.: Resilient routing in communication networks. Springer (2015)

[Sich08] Sichitiu, M.L., Kihl, M.: Inter-vehicle communication systems: a survey. IEEE Communications Surveys & Tutorials. 10(2), 88-105 (2008)

[Ster10] Sterbenz J.P.G. *et al*: "Resilience and survivability in communication networks: strategies, principles, and survey of disciplines", Computer Networks, vol. 54, no. 8, pp. 1245–1265 (2010)