Resilience in Security and Crises through Adaptions and Transitions

Timo Kalle[1], Marc-André Kaufhold[2], Franz Kuntke[2], Christian Reuter[2], Amr Rizk[3] and Ralf Steinmetz[3]

Abstract: Currently, there is a tremendous number of communication technology and systems in use. Not only in the private user space, but also in business operations and societal areas, they are deeply involved: Ranging from messaging services or navigation over (critical) SCADA systems to whole digital cities and communities. Consequently, the view on communication networks in security and particularly crisis scenarios becomes inevitable. This paper examines the notions of resilience, adaption and transition within communication networks with a specific focus on crises. Based on a structured literature review, the fundamentals of resilience and communication networks are introduced. The paper then discusses the characteristics of (a) evolvability, accessibility, usability and diversity as well as (b) self-organization, -management, -optimization, -monitoring, -healing and -protection for communication network resilience. Finally, it outlines challenges and potentials of communication network resilience based in the use cases of security and crises.

Keywords: Resilience; Communication Networks; Adaption; Transition; Security; Crisis

1 Introduction

Nowadays, communication networks are used everywhere. More and more devices with communication technology as the main feature (usually over the Internet) are used (e.g. Smartphones, Smart-TVs, Tablets) [Ka18], but also historically "dumb" tools become sensing and consequently, communicative (e.g. the navigation device with real-time traffic control or refrigerators with automatic reorders). These developments are the reason behind the drastically growing connectivity. Thus, communication networks are also growing strongly [Ci17]. While we rely more and more on connected systems since a few decades, the communication networks have become a critical infrastructure in many countries, e.g. in Germany as the critical sector "information technology and telecommunications" [Bu18]. In addition, communication networks are threatened by the paradox of vulnerability, which posits that when an always existing service fails, the disturbance by a failure is much more harmful [Bu09]. Thus, they have to be resilient since a disruption of the communication would lead to massive problems in everybody's daily life. But what does resilience mean in this context?

[1] TU Darmstadt, Multimedia Communications Lab (KOM), timo.kalle@stud.tu-darmstadt.de
[2] TU Darmstadt, Science and Technology for Peace and Security (PEASEC), {kaufhold; kuntke ; reuter}@peasec.tu-darmstadt.de
[3] TU Darmstadt, Multimedia Communications Lab (KOM), {amr.rizk; ralf.steinmetz}@kom.tu-darmstadt.de

doi:10.18420/inf2019_ws60

Resilience, defined by Laprie as “the persistence of dependability when facing changes” [La08], is a frequently used term in today’s research. Although the definition of Laprie seems to be clear, it is only used as a broad definition which is changed, refined or newly defined in different research subjects. The ambiguousness of resilience leads to the point, where some researchers define resilience as a process, whereas others see it as a property and still others talk about it as an ability [Ma16]. Many attempts were made to categorize the definitions [BJ07, CA13], also with regard to concepts such as cooperative resilience, i.e. resilience through cooperation [RLP16].

According to the aforementioned literature, resilience is dependent on the context. Thus, it can be said that there is a necessity to refine the definition according to the context, but overall, it is more important to look into the way of achieving resilience. Since the number of different definitions of resilience is enormous and the discussion about the “most perfect” definition is–in the end–not important, the focus should be more on the interplay of resilience with associated aspects. In this work, we focus on resilience in the area of communication networks with a specific focus on crises, because of the importance of this critical sector. Aspects that accompany resilience in this area are especially adaption and transition. Therefore, these two aspects are important to look at for getting an insight into communication network resilience.

The main goal of the paper is the description of the role of adaption and transition in the domain of resilient communication networks. Bringing the defined notions into the wild – with exemplary approaches in security and crises scenarios – will illustrate the prior theoretical declarations. Especially in the crises scenario, resilience is crucial and the nexus between different layer technologies will show the complexity, but also the capabilities, of modern communication systems. Also, a line-up of differences in the interpretation of the presented aspects referable to differences in the contexts of specific use cases will be constructed to clarify the basis on which the relationships rely on. At the end of the paper, the research question “What is the interplay between resilience, adaption, and transition?” (RQ1) should be answered, as well as “What are the roles of adaptions and transitions in communication network resilience?” (RQ2).

This paper is structured as follows: first, after introducing the methodology of the literature review, background information is given in Section 2 and the main paradigms are explained. They are then brought together in Section 3. In the following, these paradigms are applied to different areas of communication networks, namely security and crises, in Section 4. Subsequently, the contribution is concluded in Section 5.

2 Background

The work is based on a literature search introduced by vom Brocke et al. [Br15]. It was done sequentially, starting with an overview of the whole area of resilience and transitions. Subsequently, the literature search has been refined to focus on the important areas of resilience for this paper like the differences in communication network contexts. The

refinement process was done again when new insights revealed that further research was needed. The sources are mostly conference papers and journals extracted from bibliographic databases (ResearchGate, IEEE Xplore, ACM Digital Libraries, arXiv).

Search terms which were used are “self-x” (particularly in combination with “ICT”), “network” plus “resilience”, also enhanced with the terms “transitions” and “adaption.” While the first search for “self-x” resulted in many findings outside of the communication network context, the combination with “ICT” brought us in a fruitful direction for our topic. After the first retrieval of literature, the search keyword “transition” was used at the KOM publication website [Te18] for specific application literature. In addition, expert recommendations were used to build a good understanding of the basics in this area. Andreas Mauthe, professor and head of the research group for IT and Data Security at University of Koblenz, was consulted. His research was part of the ANA (Autonomic Network Architectures) project [CO09] and he is currently part of the Collaborative Research Centre 1053 MAKI (Multi-Mechanisms Adaptation for the Future Internet) [MA13]. The first project aimed for a novel network architecture that allows dynamic adaption and re-organization according to the working, economic and social needs of users. The latter project creates innovative approaches in communication systems that optimize the individual attributes of current network and application mechanisms to achieve flexible and robust systems. Since Andreas Mauthe was and still is a prolific project leader, he is an expert for this topic. He gave an introduction to their project’s fundamental research on communication network resilience and self-x attributes, which helped to get the needed background information.

The coverage of the research is seminal because of the tremendous amount of research in these areas, but with an attempt to be representative in the specific core topics. All searching techniques (keyword, backward and forward search) were used dependent on the examined research area. In the beginning, keyword search gave a broad overview and a lot of literature to work with. The refinement process was done especially with backward search and forward search to get more details about literature content and dependencies as well as to compare different approaches. In the end, 27 sources were considered as interesting and relevant. Seven of them were expert recommendations.

2.1 Resilience

Resilience is either broadly defined as “the capacity to recover quickly from difficulties; toughness” [St15] or defined especially for application-specific scenarios in ecological sciences, social sciences, physical domains and more. This leads to a huge number of definitions and a vague understanding of what exactly is meant when the term is used. Brand et al. [BJ07] classified the resilience definitions in three coarse-grained and subject-independent categories. The first class defines resilience in a descriptive concept, the clearest definitions are given now. Resilient systems have to have (1) the capacity to absorb disturbances, (2) the ability of self-organization and (3) the possibility of learning and adaption. Resilience is “a measure of the persistence of systems and of their ability

to absorb change and disturbance and still maintain the same relationships between (...) variables" or "the transition probability between states as a function of the consumption and production activities of decision-makers". In the second class, resilience is defined as a normative concept. Resilience is the "flexibility over the long term" or the "maintenance of natural capital in the long run". The third class is a hybrid concept of both previous classes with definitions like "the capacity of a (...) system to absorb recurrent disturbances (...) so as to retain essential structures, processed and feedbacks".

The CARRI report [CA13] gathered many resilience definitions and understandings. An old but still viable definition is from Holling [Ho73]: "The persistence of relationships within a system; a measure of the ability of systems to absorb changes of state variables, driving variables, and parameters, and still persist." Klein et al. [KNT03] defined resilience as "the ability of a system that has undergone stress to recover and return to its original state; more precisely (i) the amount of disturbance a system can absorb and still remain within the same state or domain of attraction and (ii) the degree to which the system is capable of self-organization." Here, we can clearly identify a similarity to the first definition in the descriptive class of Brand given above, but without the learning possibility. The CARRI report also gives the definition of the Resilience Alliance from 2009: "The capacity of a system to tolerate disturbance without collapsing into a qualitatively different state that is controlled by a different set of processes," which focused clearly on the quality outcome of a system. Lastly, Butler [BML06] sees resilience as "good adaption under extenuating circumstances; a recovery trajectory that returns to baseline functioning following a challenge."

Further approaches aim to measure resilience. A general principle in quantifying resilience is the 3-D Resilience Framework [Bé12], where resilience is the result of three capacities and each capacity leads to a different outcome. The absorptive coping capacity has small transaction costs and low intensity of change. The outcome of this capacity is the persistence. The counterpart is the transformative capacity, where the intensity of change is high as well as the transaction costs. The outcomes are transformational responses. Between these capacities is the adaptive capacity with flexibility in change/costs and incremental adjustment as the outcome. Although the approaches of quantifying resilience are unusable in real world contexts, it is interesting that they already differentiate between "adaptive" and "transformative".

In addition, it is important to mention that resilience involves uncertainty. Similar to business research, we divide uncertainty in two separate types [Kn64]. On the one hand, we have the uncertainty risk, when probabilities for results are known or if they can be named or framed. On the other hand, we have (genuine) uncertainty, when there is no a priori knowledge about results. This differentiation is important when resilience in systems is evaluated as both types are diverse in terms of complexity.

2.2 Communication Networks

Communication networks evolved into one of today's most important factors in daily life. Many different networks exist, like the well-known telephone network with its typical unicast connection or the Pan-European Network Service, a special network for Air Navigation Service Providers. Other widely used networks are radio networks, usually used for broadcast services or two-way communication over handheld transceivers and television networks, which evolved from the audio-only transmissions of the radio and made video broadcasting possible. The uncontested most important communication network is the Internet. Started as a military network, the ARPANET (Advanced Research Projects Agency Network), it is now a global interconnection between billions of computers, servers and devices, roughly grouped in sub-networks.

In Cisco's White Paper "The Zettabyte Era" [Ci17], the importance of coping with the future Internet is displayed with numbers. The number of devices and connections are growing faster than both the population (1.1%) and Internet users (7%) with 10% compound annual growth rate. While the number of devices was already above 16 billion in 2016, they broke through the 20 billion margin in 2018 and will most likely reach 26+ billion in 2021. In Western Europe, the average number of devices and connections per capita was at 5.3 and in North America even at 7.7 in 2016, which shows that the modern society progression goes hand in hand with networked devices. In [Al19], it is stated that in the future Internet – where the exchange of data is subject to the dense connectivity dynamics and nowadays high-quality requirements – transitions are crucial to cope with the challenges which arise today or will arise in the future.

Another important point is to distinguish the meanings of transition and adaption. Usually, they are used in an ill-defined way to describe quite similar circumstances. We differentiate them now precisely for the purpose of this research. A look into the Oxford dictionary [St15] gives us the on-point definition for a transition: "The process or a period of changing from one state or condition to another." This can be directly used for the communication network as "the process of changing from one system state or system mechanism to another system state or mechanism," while the system in our case is the overall communication system. Therefore, a state change would include scenarios like a change from one network stack protocol to another one (e.g. from TCP to UDP) or the change of the physical layer link which a device is using (e.g. from LTE to Wi-Fi) [Ri17]. In [Fr16], the concept of transitions is defined as "the functional replacement of a mechanism by a functionally similar or equivalent other mechanism in a running communication system without causing an error." In addition, it is apparent that various mechanisms perform differently under varying environment characteristics, showing that the context is of utmost importance in today's dynamic communication networks.

A general visualization for transitions is given in Fig. 1. We consider different mechanisms (1-3), which can achieve a specific communication quality (y-axis) in different environment conditions (x-axis). A system that uses transitions can switch between these mechanisms to sustain a high and steady quality in dynamic environments (red line). A

"single mechanism system" would suffer under a dynamic environment because the mechanism can only achieve a good quality in the environment it is built for (black solid/dashed/dotted line).

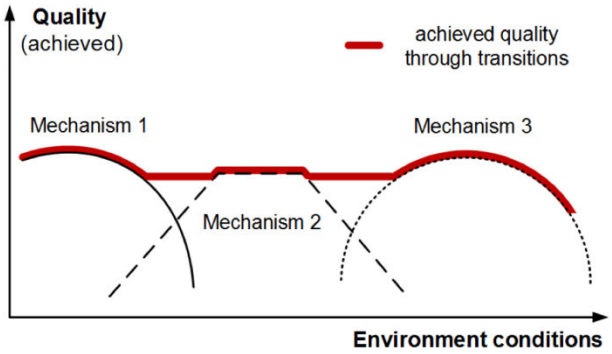

Fig. 1: Transitions between three different mechanisms and the improved quality, from [MA13]

Adaption, by definition "the action or process of adapting or being adapted," needs a closer look too. We can refine the definition by looking up the definition of adapt ("Make (something) suitable for a new use or purpose; modify") or using a subject-specific definition e.g. the biological definition: "The process of change by which an organism or species becomes better suited to its environment" [St15]. By replacing organism or species with system or technology, we obtain a computer scientific approach. It is important that the adaption logic, as well as transitions in communication systems, has a feedback control loop to sense the environment and react to context changes. A well-defined approach for this control loop is the MAPE principle with the phases of monitoring the environment and the inner system state, analyzing the sensed data, planning the next step the system will take, and executing the planned action [Br09]. Understanding the adaptation logic in communication systems becomes more important. Tools for self-adaptive communication systems, which visualize the system's adaptation behaviour, were built recently to encounter the complexity [Pf19].

Overall, we have to differentiate clearly between adaption and transition. Both are triggered by special circumstances or environmental changes, but while transitions need the coexistence of different technologies so that there can be a changeover from one mechanism to another mechanism, an adaption is a finer-grained adjustment inside a mechanism itself. Thus, an adaption is a "small step" inside a mechanism (e.g. a parameter adjustment inside of an algorithm) and in a transition, there is the complete mechanism changed which is, therefore, a coarse-grained adjustment (e.g. the replacement of the currently used algorithm by an alternative one).

3 Communication Networks Resilience

Communication networks have specific characteristics which have to be kept in mind when making them resilient. What are the properties a resilient communication system should have? Laprie's approach [La08] fits well in this area. It is said that resilience can be achieved by looking into four dimensions of a system.

1. Evolvability is needed to successfully accommodate to changes. The system has to be dynamic to be able to react to environmental changes as well as changes within the system itself. Adaptivity, e.g. as the capability of evolving while executing, is represented to be an important a sub-property of evolvability. In communication networks, this would be for example the pervasive change of used underlying physical network communication without an interruption of the overall network.
2. Assessability is necessary for justified confidence in the system. The system status should be perceptible for people and a certain amount of transparency is needed for an understanding of the system's decisions. Also, keeping track of the system behaviour brings confidence because then there is always the possibility of analyzing the past actions of a system in detail. In the context of communication networks, this means that the current (and previous) connection states, as well as the used communication technologies, are exposed to the user.
3. Usability is also important as it is a key factor in every technology where interaction appears. Communication networks have an indirectly important need for usability as it is an extraordinary important concept for every application, device and other component in this context.
4. Diversity prevents problems with single point of failure. By nature, most communication networks are highly heterogeneous because there is always a very high number of different components and devices in use. Still, this property should be kept in mind explicitly when communication networks are built or investigated.

Another approach for system properties uses the "self-x attributes" [Ma13]. A perfect communication network relying on self-x would be self-organizing, self-managing, self-optimizing, self-monitoring, self-healing and have self-protection. Yet it has to be kept in mind that "self-x" can have a different meaning in other contexts.

- Self-organizing means that nodes within the network organize themselves to form a community with dynamic role assignment to nodes and joint decision making.
- Self-managing systems have nodes that manage their behaviour according to context and rules. This implies that the system is able to self-configure so that manual configuration is not needed.
- Self-optimizing intends that the network adapts the node behaviour to regular network conditions. This leads to a global optimization via joint decision making.

- Self-monitoring systems have nodes which monitor their own state. Through the observation of neighbour node behaviour, the overall system achieves network state awareness. These systems have to have the ability of information sensing and processing for this property.
- Self-healing is the ability to recover from node failures through network re-organization. After a fail, nodes can recover through re-configuration.
- Self-protection puts the focus on security. The system should be able to protect itself against attacks and malicious behaviour.

There are relations between the properties of Laprie/the self-x attributes and the paradigms of adaptions and transitions. The most obvious one is that evolvability is only possible when the communication network is adaptive. Although adaptivity is declared a sub-property of evolvability, it is also mentionable that it is the most important property. In the scope of Laprie, transitions would be also a part of the adaptivity property. For assessability, the relation is not as obvious as before. Here, the adaptions would be needed to change the insights of the system, e.g. by changing the data that is represented. A system with this capability can be analyzed in an easier way, leading to the understanding of the system's actions and overall confidence. Usability comes hand in hand with adaptions, too. As with adaptions, there is the possibility to adjust the system or its components to the user's needs, it is more likely that system usability is given. Transitions are the key factor to work with diversity. Whenever the system is able to change single mechanisms within itself or if the system supports many kinds of heterogeneous devices by design, the system gains diversity. The self-x attributes are related to transitions and adaptions in a more straightforward way: As every attribute is relying on the factor that the system itself – without any manual or external actions – decides on what to do and when to do, it has to cope with the complete environment as well as with its inner state. As already known, both of these aspects are highly variable and dynamic and thus they have to utilize adaptions and especially transitions.

In sum, achieving these properties is most likely possible, or only possible, through adaptions and transitions. Also, there are many different concepts, technologies and designs for future communication networks. At a first glance, it seems to make it easier for achieving resilience when there are so many approaches. In the end, it makes the problem more complex since the decision space for the system grows as well. In general, different fields of operation for communication networks have to be investigated to understand dissimilarities in their way of gaining resilience.

4 Use Cases in Communication Networks

In the following subsections, we apply the above-explained paradigms onto the use case scenarios of resilience in security and crises.

4.1 Resilience in Security

Resilience from the security point of view requires a range of resilience mechanisms, as expert recommendations from the ANA Project explains. These are usually built for specific parts of a system, placed across various layers of the protocol stack and used for different administrative domains. Since the networking infrastructures are usually heterogeneous, different mechanisms are needed for different devices. Therefore, many smaller resilience mechanisms are needed to gain overall resilience. These can be partitioned into two categories: detection and remediation mechanisms. While the job of the detection mechanism is the identification and categorization of a monitored system or environment behaviour, the remediation mechanism implements functions for the mitigation of threats, attacks and failures. During run-time, a system should be able to learn from past scenarios by discerning reusable patterns for resilience [Sc14]. Such a system should be able to learn in an offline simulation, where known resilience strategies to combat specific types of challenges are inserted. In addition, evaluation of, e.g. policy-based, configurations of mechanisms would lead to transparency, which is needed because security or resilience technologies should not be used as a black box. The output of the simulation should be generalized successful solutions, called resilience patterns. These patterns specify possible policy-driven configurations between a set of abstract mechanisms types and their behaviour. At last, the challenge analysis takes place. It is the online part of the system to cope with uncertainty in new situations. Online monitoring is used to gather and store information about the current state of the network. Appropriate patterns are selected and deployed when challenges are observed during the runtime of the system. Overall, there is a permanent feedback control loop in the system and combinations of different resilience mechanisms and policies are brought together to strengthen overall system resilience out of many partly resilient mechanisms.

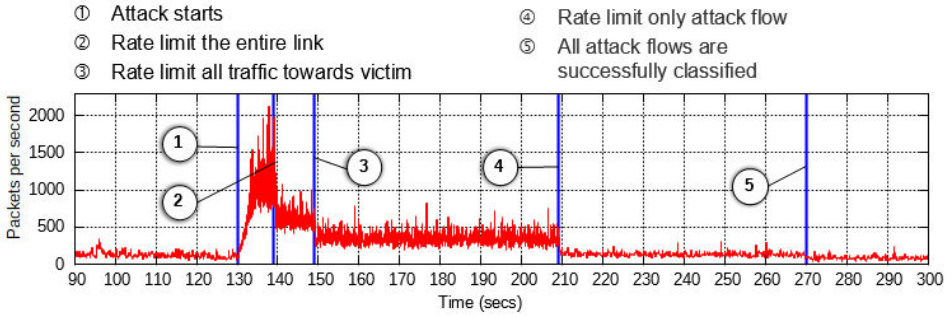

Fig. 2: Example DDoS use case for resilience in communication network security

In [Sc14], network resilience is formed by using reusable management patterns. The difficulty lies in decision-making with the correct interpretation of the situation. The system has to be adaptive as every attack is unique and changes between different reaction mechanisms have to be made. An example with a DDoS attack is shown in Fig. 2. The attack starts (1) and after 10 seconds, the entire link is limited to a certain rate to

prevent a service shutdown (2). Then, the victim is identified and only the link towards the victim is limited. Other links are released (3). It takes some time until the attack flow is identified and limited (4) and after ~140 seconds, all attack flows are classified and can be handled (5). While it seems to be a long time from the start of the attack until it is defended (over 2 minutes), it takes less than 20 seconds until most traffic in the network is working without service disruptions and the disturbance is mitigated to a minimum.

Overall, resilience in the area of security is difficult to achieve and should be paid attention to in the future. Nowadays, through developments like the Internet of Things (IoT) and smart cities, there is an exponential increase of potential attack points and points of failure [KD19]. These problems could be tackled by best-effort approaches like the Swiss cheese model, where many security layers are used to create a secure environment, but "overlaying" flaws in each layer can lead to possible security breaches. Thus, security-by-design and resilience-by-design principles should be used.

4.2 Resilience in Crises

In crises, resilience is seen as the ability to withstand exposed dangers, to absorb them and to recover from the effects on time and in an efficient manner. This happens through the preservation and restoration of the essential basic structures and functions of the respective system. Even if actors in damage situations like to return to a previous state, especially in the context of disasters, sometimes it is not possible to build up the previously used infrastructure again [Re18]. In communication networks, new ways have to be found to communicate over short to long distances. However, because communication networks are always available in modern countries, a breakdown can have a huge negative impact with unforeseen cascading effects.

A responsive emergency communication network architecture [Li17] shows the different leverage points for transitions and adaptions in these crisis scenarios, when the currently used communication networks collapsed and thus are not available for communication. New ways for communication have to be found for generating short-term resilience. While fast to build basis networks for organization to organization (O2O) and organization to civilian (O2C) communication exist for a while now, new approaches rely civilian to civilian (C2C) and civilian to organization (C2O) communication due to the rise of smartphone and social media – despite sometimes chaotic – use during crises [Ka19]. These different communication scenarios require transitions between different approaches as civilians and organizations' staff have different knowledge about important factors in disasters. Examples of different C2C/C2O approaches are Twimight which enables Bluetooth communication for Twitter users and SOS-Cast which broadcasts an SOS message to the nearest device to reach an organizational person (via hop-by-hop communication). Other approaches like Several Mesh build up a new delay-tolerant network based on mobile ad-hoc networks. After and during disasters, civilians require different services such as "I am alive"-notifications and its counterpart "person-finder,"

SOS-emergency messages, situation assessment, information/news services, tasking services for self-organizing groups of civilians and lastly, messaging services.

These services require different forms of dissemination. Thus, transitions between unicast, broadcast, multicast, geocast or anycast communication are inevitable. Further, the whole communication protocol should be changeable because different protocols provide different network service qualities, e.g. best effort or reliable communication, connectionless or end-to-end, with error detection or without and many more. On the physical layer, the transmission technology should be also transitional simply because some technologies could be unusable. While today the physical layer technologies are already adaptive to small changes in the environment, they can still crash and transitions to an equivalent transmission technology would be needed (e.g. from Wi-Fi-Direct to Bluetooth or radio waves). An emerging technology, which is particularly deployed in Smart Cities nowadays, is the Long Range Wide Area Network (LoRaWAN) [RKS17]. This technology does not substitute but complements the cellular networks used today. While this seems to be a redundant technology at first, it is used to get a better-suited network for the IoT paradigm on the one hand, and to have an alternative network when the cellular network does not work. Also, it has a higher physical penetration, e.g. to get connections in underground infrastructures like basements. Hence, it enables another distribution channel for emergency messages from or to public authorities.

When – on application layer – going deeper into the messaging service, new problems arise, like the prioritization of messages. During the resilience process in a post-disaster scenario, the prioritization will change simply because the needs change. To provide an example: While at first after an earthquake, messages of lost or wounded people have to be prioritized, logistical resource information messages will become more important after some time. Services need to be adaptable to these context changes. Also, these prioritization approaches improve the agility of communication systems and lead to more efficient behaviour. In crises scenarios, transitions between different mechanisms are even more important due to the hard context changes which appear in every possible layer of communication networks. Nevertheless, adaptions are also needed to ensure the stability of the different mechanisms within lasting – but unstable – context states.

5 Conclusion

Resilience is important and especially in critical infrastructures like communication networks, it is a crucial characteristic. For gaining resilience, the concepts of adaptions and transitions should be used and the differences between them should be known. RQ1 (“What is the interplay between resilience, adaption, and transition?”) can be answered with Fig. 3, showing the relationships between resilience, adaptions, and transitions. Resilience needs either transitions or adaptions (or both), depending on changes in context. For small changes, adaptivity is needed (e.g. algorithm parametrization). For substantial changes, transitions are the right concept (e.g. algorithm replacement). If small

and substantial changes are observed, both concepts are needed, but then they need coordination between each other.

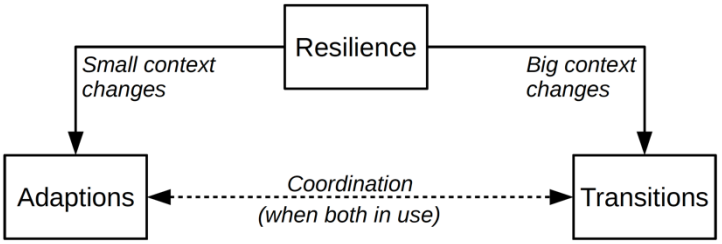

Fig. 3: The final relationship representation of the concepts described in this paper

With regard to RQ2 ("What are the roles of adaptions and transitions in communication network resilience?"), there is no generic answer simply because the roles are highly dependent on the context. They vary in their applicability in different use case scenarios as well as the depth of the network layer in which they are used. Overall, both concepts are required but they have to be coordinated because they are not independent. While these circumstances are usually known, we add another important and newer condition: Transitions have to be resilient themselves. This is important, because only when every used transition is itself resilient, the system is always and provably in a desired and secure state. Finally, the roles of adaptions and transitions for communication network resilience are very important, but their composition has to be formed dependent on the context. A detailed analysis of the use case scenarios, threats and hazards is crucial. Then, it will be clear if the system should be more transition-based or very adaptive.

This paper is subject to limitations and offers potential for future research: To draw an in-depth picture on resilience in communication networks, definitions and standards by organisations such as NIST, ISO and OASIS have to be examined in detail. Since recommendations were proposed by a single expert, multi-perspective workshops should be conducted to meet the interdisciplinary character of resilience and add empirical evidence. Based on more elaborate foundations, research has to provide implementation paths for crisis informatics [RK18] and in security-critical domains [Re18].

Acknowledgements: This work has been funded by the DFG as part of projects X3 and C3 within the CRC 1053 MAKI.

Bibliography

[Al19] Alt, B. et al.: Transitions: A Protocol-Independent View of the Future Internet. In: *Proceedings of the IEEE* vol. 107 (2019), Nr. 4, pp. 835–846

[Br09] Brun, Y. et al.: Engineering Self-Adaptive Systems through Feedback Loops. In: *Self-Adaptive Systems*, 2009, pp. 48–70

[BJ07] Brand, F.S.; Jax, K.: Resilience as a Descriptive Concept and a Boundary Object. In: *Ecology and Society* vol. 12 (2007), Nr. 1

[Br15] Brocke, J. et al.: Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. In: *Communications of the Association for Information Systems* vol. 37 (2015), pp. 205–224

[BML06] Butler, L.D.; Morland, L.A.; Leskin, G.A.: Psychological Resilience in the Face of Terrorism. In: *Psychology of Terrorism* : Oxford University Press, 2006, pp. 400–417

[Bu09] Bundesministerium des Inneren: *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*. Berlin, 2009

[Bu18] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: *Critical Infrastructures divided by sectors and subsectors*. https://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html. Retrieved: 2019-06-12

[Bé12] Béné, C. et al.: Resilience: New Utopia or New Tyranny? Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes. In: *IDS Working Papers* vol. 2012 (2012), Nr. 405, pp. 1–61

[CA13] CARRI: *Definitions of Community Resilience: An Analysis*. http://www.resilientus.org/about-us/what-is-community-resilience/. Retrieved: 2019-06-12

[Ci17] Cisco: *The Zettabyte Era: Trends and Analysis*. https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html. Retrieved: 2019-06-12

[CO09] CORDIS: *Autonomic Network Architectures*. https://cordis.europa.eu/project/rcn/80655/factsheet/en. Retrieved: 2019-06-12

[Fr16] Frömmgen, A. et al.: *Mechanism Transitions: A New Paradigm for a Highly Adaptive Internet*, 2016

[Ho73] Holling, C.S.: Resilience and Stability of Ecological Systems. In: *Annual Review of Ecology and Systematics* vol. 4 (1973), Nr. 1, pp. 1–23

[Ka19] Kaufhold, M.-A. et al.: Avoiding chaotic use of social media before, during, and after emergencies: Design and evaluation of citizens' guidelines. In: *Journal of Contingencies and Crisis Management* (2019), pp. 1–16

[KD19] Kitchin, R.; Dodge, M.: The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. In: *Journal of Urban Technology* vol. 26 (2019), Nr. 2, pp. 47–65

[KNT03] Klein, R.J.T.; Nicholls, R.J.; Thomalla, F.: Resilience to natural hazards: How useful is this concept? In: *Environmental Hazards* vol. 5 (2003), Nr. 1, pp. 35–45

[Kn64] Knight, F.: *Risk, Uncertainty and Profit* : Reprints of Economic Classics, 1964

[Ka18] Kaufhold, M.-A. et al.: 112.social: Design and Evaluation of a Mobile Crisis App for Bidirectional Communication between Emergency Services and Citizens. In: *European*

Conference on Information Systems (ECIS). Portsmouth, UK : AISeL, 2018

[Li17] Lieser, P. et al.: Architecture for responsive emergency communications networks. In: *2017 IEEE Global Humanitarian Technology Conference (GHTC)* : IEEE, 2017, pp. 1–9

[La08] Laprie, J.-C.: From Dependability to Resilience. In: *International Conference on Dependable Systems and Networks*, 2008, pp. G8–G9

[MA13] MAKI: *Sonderforschungsbereich 1053 – Multi-Mechanismen-Adaption für das künftige Internet*. https://www.maki.tu-darmstadt.de/sfb_maki/ueber_maki/index.de.jsp. Retrieved: 2019-06-12

[Ma13] Mauthe, A.U.: Resilience in Autonomic Networking Architectures. In: *MAKI Seminar TU Darmstadt*, 2013

[Ma16] Mauthe, A. et al.: Disaster-resilient communication networks: Principles and best practices. In: *Proceedings of 2016 8th International Workshop on Resilient Networks Design and Modeling, RNDM 2016* vol. 8 (2016), Nr. 1, pp. 1–10

[Pf19] Pfannemüller, M. et al.: CoalaViz: Supporting Traceability of Adaptation Decisions in Pervasive Communication Systems. In: *2019 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops*, 2019

[RKS17] Raza, U.; Kulkarni, P.; Sooriyabandara, M.: Low Power Wide Area Networks: An Overview. In: *IEEE Communications Surveys & Tutorials* vol. 19 (2017), Nr. 2, pp. 855–873

[RK18] Reuter, C.; Kaufhold, M.-A.: Fifteen Years of Social Media in Emergencies: A Retrospective Review and Future Directions for Crisis Informatics. In: *Journal of Contingencies and Crisis Management (JCCM)* vol. 26 (2018), Nr. 1, pp. 41–57

[RLP16] Reuter, C.; Ludwig, T.; Pipek, V.: Kooperative Resilienz – ein soziotechnischer Ansatz durch Kooperationstechnologien im Krisenmanagement. In: *Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie (GIO)* (2016)

[Re18] Reuter, C.: *Sicherheitskritische Mensch-Computer-Interaktion Interaktive Technologien und Soziale Medien im Krisen-und Sicherheitsmanagement*: Springer Vieweg, 2018

[Ri17] Richerzhagen, B.: *Mechanism Transitions in Publish/Subscribe Systems: Adaptive Event Brokering for Location-based Mobile Social Applications*, Technische Universität Darmstadt, 2017

[Sc14] Schaeffer-Filho, A. et al.: Network resilience with reusable management patterns. In: *IEEE Communications Magazine* vol. 52, IEEE (2014), Nr. 7, pp. 108–115

[St15] Stevenson, A.: *Oxford Dictionary of English* : Oxford University Press, 2015

[Te18] Technische Universität Darmstadt: *Multimedia Communications Lab*. https://www.kom.tu-darmstadt.de/research-results/publications/. Retrieved: 2019-06-12