A Framework for Spatial and Temporal Evaluation of Network Disaster Recovery

Marija Gajić*, Marija Furdek†, Poul Heegaard*
* Department of Information Security and Communication Technology
NTNU - Norwegian University of Science and Technology
{marija.gajic|poul.heegaard}@ntnu.no
† Department of Electrical Engineering, Chalmers University of Technology, Sweden
furdek@chalmers.se

***Abstract*—The support of vital societal functions requires a reliable communication network, especially in the presence of crises and disastrous events. Disasters caused by natural factors including earthquakes, fires, floods or hurricanes can disable network elements such as links and nodes and cause widespread disruption in end users connectivity to network services. Effects of disasters can vary over space and time due to disaster escalation and propagation. Network recovery from disasters requires understanding of both the spatial properties of the hazard at hand, and their temporal evolution. While the former has already been addressed in the literature, existing models and measures are unable to capture the temporal aspects of disaster recovery.**

This paper proposes a framework for spatial and temporal evaluation of network disaster recovery. It allows for modelling random spatial patterns of disasters in a geographical grid. The temporal aspects captured in our framework include changes due to the progression of a potentially shape-changing disaster across the affected area, as well as to the recovery actions of adaptive network reconfiguration and topology reconstruction undertaken by the network operator. The framework applicability is demonstrated on a content delivery network use case example, where we capture the evolving network performance in terms of the average shortest path length between the peers and the content replicas hosted by servers. By providing insights into the spatial and temporal effects of both disaster escalation and remediation measures, our proposed framework lays down the groundwork for flexible disaster modelling and recovery sequence optimization.

***Index Terms*—Survivability, disaster recovery, network resilience, content delivery network.**

I. Introduction

For normal functioning, our society is steadily more dependent on a reliable, high-performance communication network supporting access to vital services. Uninterrupted connectivity to network services and content is particularly important in times of crises and disastrous events such as sabotage, natural disasters, massive hardware failure, common and propagating software failures and cyber-attacks. These can have massive consequences on the network infrastructure, i.e. nodes, links and servers. To counteract such events and recover the network in a quick and efficient way, a deep understanding of the impact of both the disasters and the various remediation actions is necessary. To capture the effects of a disastrous event, we need a method for instantaneous assessment of the non-functional properties of the service, such as *performance* (e.g. peer to server request delays), and *dependability* (e.g. fractions of peers connected to a server), but also how these properties change over time until the system is fully recovered.

After an initial disastrous event occurs, its consequences might evolve over time due to:

1) Propagation and escalation, e.g., a disaster affecting another/larger part of the (embedded) system or a high intensity disaster triggering a new follow-up disaster, and
2) System reconfiguration, repair, and service restoration.

Therefore, to fully assess the consequences of the event both their spatial and temporal aspects should be considered. The *spatial* dimension refers to the extent of the event's consequences (e.g., how many nodes and links in the networks are destroyed and need to be repaired) and their evolution over the affected area. The *temporal* dimension concerns the consequences' duration (e.g., how long it takes to repair all links that are cut) and their evolution over time.

In the *survivability* quantification framework proposed in [1], the idea is to construct a meta model which captures the different phases after the initial impact. A *recovery phase* is a (discrete) change in the system state (system configuration and service delivery), caused by potential event escalation or propagation, in addition to recovery actions (e.g., connection rerouting, relocation of servers, link or node repair).

In this paper, we develop a model for jointly capturing the spatial and temporal dimensions of a disaster and remediation actions. Our framework can model a variety of disaster types with spatial and temporal variations. We demonstrate the applicability of the framework in a content delivery network affected by a disaster. The use case example aims at showing the importance of considering both the spatial and temporal dimension of a disastrous event and remediation steps to get additional insights compared to only considering the immediate impact.

This work was supported by the Swedish Research Council project "Safeguarding Optical Communication Networks from Cyber-Security Attacks" and COST Action 15127 RECODIS.

Examples of consequences considered in our survivability quantification framework include:

1) Instantaneous initial impact (spatial)
2) Accumulated impact on the service over time (spatial and temporal)
3) Worst case situation, peak consequence (spatial)
4) Recovery time (time it takes to restore a critical service or certain percentage of a service of interest, or until it is fully recovered)

We define metrics that quantify the consequences described above. This will add insights to the survivability of a system affected by different undesired events which develop from their initial impact. Furthermore, the insights will enable a quantifiable comparison between various strategies to handle such disastrous events.

The paper is organised as follows. Section II reviews the relevant related work from the literature. Section III describes the survivability quantification framework, including the representation of network topology with server assignment, and instantaneous, propagating and escalating disasters. Section IV describes disaster recovery strategies including peer-server (re)connection, replica relocation/instantiation and link repair. A use case scenario of propagating disaster demonstrating the applicability of the framework is introduced in Section V, before the closing remarks in Section VI.

II. Related Work

Resilience and survivability of networked systems have been extensively studied in the literature. The vast body of literature relevant to our work can be roughly systematized according to four main aspects: modelling and definitions of fundamental concepts, disaster impact modelling, disaster-aware network design and provisioning, and disaster recovery.

An exhaustive overview of basic concepts and taxonomy of definitions related to system dependability in the presence of various faults is presented in [2]. In [3] and [4], the authors refine the definitions related to network disruption tolerance and investigate the practical implication to its modeling and quantification. The *survivability* quantification framework in [1] considered phased time recovery without taking into account the disaster escalation and propagation. In [5], the framework from [1] is applied to model (simplistic) disaster propagation and study the consequences on a wireless network.

In [6], [7], [8], approaches for geographical modelling of (correlated) failures are proposed. These models can be categorized into two types: i) deterministic failures which consider circular regions where the failure probability is one inside, and zero outside the region, and ii) probabilistic failures where the failure probability inside the region monotonously decreases with the distance from the failure epicenter. Such circular representation of the failure region, and the constant probability of failure between two consecutive concentric annuluses constrain the flexibility of a disaster model representation.

Network vulnerability to disasters can be reduced by incorporating the knowledge of disaster effects into various phases of network life cycle, such as disaster-aware network design and provisioning or post-disaster recovery. Approaches for strategic placement of network links and nodes aimed at increasing resilience to man-made infrastructure attacks can be found in [9]. Approaches for disaster-resilient design of datacenter networks are presented in [10], while the placement of replicas across distributed cloud networks resilient to targeted fiber cuts is investigated in [11].

Network resilience in the presence of certain types of disasters (e.g. hurricanes) may also benefit from the forecasts and trajectory projections. Alert-based migration of virtual machines to safer datacenter is performed in [12]. The work in [13] combines the awareness of both disaster impact and remediation in terms of content evacuation and incorporates it into the datacenter placement. Approaches for joint progressive post-disaster network and datacenter recovery are investigated in [14]. While the vast majority of aforementioned works addresses the various aspects of disaster modeling and post-disaster recovery, they are unable to capture the evolving spatial and temporal effects of disaster propagation and remediation actions.

III. Modelling Framework

This section describes the modelling framework used to capture both the spatial and temporal consequences of a disastrous event on the network infrastructure. The main idea is to model the stages from the initial disastrous event (enforced) until the system is fully recovered. For each stage, the network topology and peer-server associations will change due to disaster escalation/propagation, and relocation/repair. For this we need the following:

- *Coordinate system* - a two-dimensional xy-coordinate system, $\Omega = \{(x, y)\}$.
- *Network topology* - the network consisting of nodes and links with connected peers and servers is defined as a graph G mapped on the coordinate system Ω. The graph on Ω with the peer-server associations (routing) defines the state of the system.
- *Disaster area* - the (immediate and evolved) area, $\mathcal{D}$ impacted by the disastrous event, mapped onto Ω
- *State of network topology* - the network topology $G_x \subseteq G$ in state x
- *Metrics* (rewards) - is a reward rate function of the network topology, $M_x = \mathcal{R}(G_k)$ in state x
- *Recovery strategies* - (best possible) relocation and/or repair actions which change the state of G such that performance and dependability of the network are improved.
- *Survivability quantification framework* - obtains the probabilities $p_x(t)$ of observing the network in state G_x time t after the event, and combines this with the rewards M_x to obtain spatial and temporal consequences of the disastrous event.

A. Survivability quantification definition

In this paper we use the definitions of *survivability* from [1]

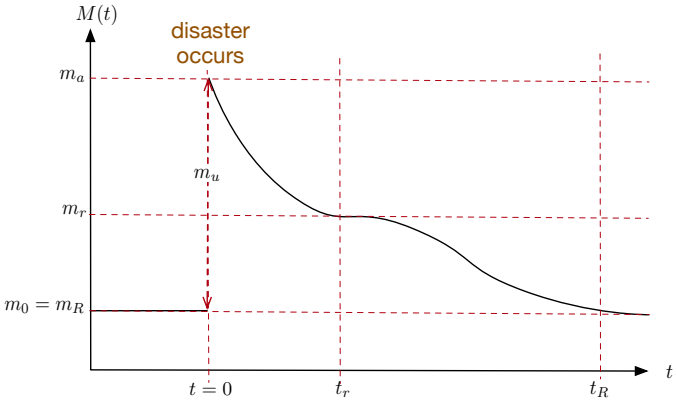

Fig. 1: Survivability after first failure [16].

> *Survivability* is the *system's* ability to continuously deliver *services* in compliance with the given *requirements* in the presence of failures and other *undesired events.*

An undesired event is a disastrous event, such as sabotage, natural disasters, massive hardware failure, common and propagating software failure or cyber-attacks, having huge consequences on the critical infrastructure.

To quantify the surviability we use the definition given by ANSI T1A1 [15], and the modelling approach from [1], [16].

> *Survivability quantification*. The measure of interest M has the value m_0 just before a failure occurs. The survivability behavior can be depicted by the following attributes: m_a is the value of M just after the failure occurs; m_u is the maximum difference between the value of M and m_a after the failure; m_r is the restored value of M after some time t_r; and t_R is the relaxation time for the system to restore the value of M.

Note that without loss of generality we assume that the larger M the poorer the system is.

These attributes are illustrated in Figure 1. The measure of interest M will in this paper be performance metrics such as the *number of connected peers to a server* or *path length and delay from peers to server* (infinite if not connected). The changes in system performance, $M(t)$, from immediately after the occurrence of a disaster (at $t = 0$) and throughout the stages of the recovery can be analyzed using this approach.

B. Coordinate system

A two-dimensional coordinate system for the considered geographical areas $X \times Y$ is defined as,

$$\Omega = \{(x, y)\} \;\; (x = 1, \cdots, X, \;\; y = 1, \cdots, Y)$$

To enable shortest path routing on Ω the coordinates (x, y) are linked to its neighbor nodes, which are assigned non-zero weights for all coordinates one step away (including the diagonals), i.e.,

$$w_{i,j} = \begin{cases} > 0 & : \; i = (x, y) \texttt{ and } j = (x \pm 1, y \pm 1) \\ 0 & : \; \texttt{otherwise} \end{cases}$$

The granularity of the coordinate system can be adjusted such that each coordinate refers only to at most one node or one link segment as introduced below. See Figure 2 for an illustration of the layout of the coordinate system. By assigning different weights on $w_{i,j} > 0$ we may model natural obstacles (lakes, rocks, buildings, etc.) to be avoided (by setting a higher cost) when planning the cable ditches (e.g., by shortest path routing). The coordinate system might be extended by a third dimension to model a 3D topology of the geographical area.

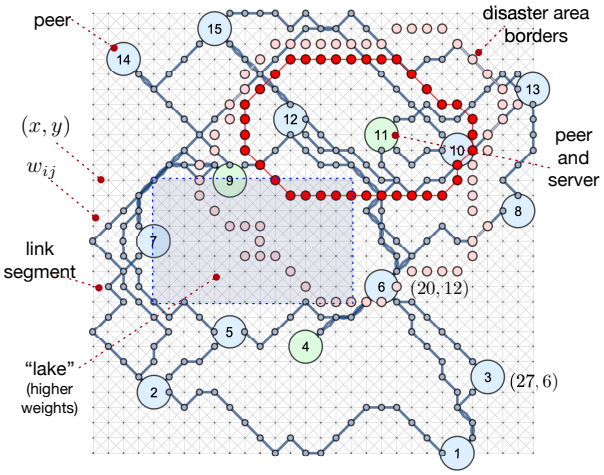

Fig. 2: Example of a network with $V = 15$ nodes (blue and yellow), $E = 23$ links (gray), and $s = 3$ servers (yellow), with two disaster areas (red and light red) mapped onto a 30×30 coordinate system.

C. Topology model

A network consists of nodes V and links E, with connected peers $U = V$ (all nodes are peers) and servers $S \subseteq V$ (N_s is the number of servers), and is represented as a graph, $G = \{V, E, S\}$ mapped onto the coordinate system Ω. The N_V nodes are represented by their coordinates, $V = \{(x_i, y_i)\}$, $i = 1, \cdots, N_V$, and the set of N_E links E is represented by the coordinates of the path of link segments that constitute the link.

The network topology example in Figure 2 illustrates the mapping of the nodes and links in graph G onto a $\Omega_{30\times30}$ coordinate system. Nodes are described as light blue and light green (servers) circles ($n = 15$), while links are represented with blue lines. As an example, link 1 which is connecting the nodes V_3 (coordinates $\{(27, 6)\}$) and V_6 (coordinates $\{(20, 12)\}$) is described by the following set of coordinates of the endpoints of the link line segments: $E_1 = \{(27, 6), (26, 7), (25, 8), \cdots, (20, 12)\}$.

D. Disaster model

A disaster area $\mathcal{D}$ is mapped onto the same coordinate system Ω, i.e., the area is represented by its (x, y)-coordinates. The disaster area might change over time, can have different shapes and sizes, and its impact on G depends on the nature of the considered disastrous event. The event impact intensity is modelled as a probability $p_{G,\mathcal{D}}$ of node or link failures of G in the area $\mathcal{D}$.

A disaster area that manifests itself at time t and changes the graph to G_x is denoted $\mathcal{D}_{x,t}$. Modelling of dynamics (propagation, decay, and escalation) of the disastrous events, requires both temporal and spatial dimensions. We distinguish between three categories of disastrous events:

1) *Single-hit disasters* - These disasters have a central area where the disaster is most powerful. Areas around this central region could also be affected but with considerably less intensity. One example of a single-hit disaster is an earthquake being the strongest in the epicenter area. Such an event has an immediate impact in a specific area, with different intensity around the central epicenter. To model this, the disaster area is discretized in K sub-areas $\mathcal{D}_{k,0}$ with different failure probability

2) *Propagating disasters* - Propagating disasters is a category embodying dynamic disasters such as hurricanes, tornadoes or fires which move across several regions with certain propagation speed. This is modelled as multiple disaster areas with different epicenter and size, which will change over time, as well as the failure probability for each area

3) *Escalating disasters* - Disasters with secondary effects are correlated disasters happening either simultaneously or one after another in a cause-and-consequence co-relation (e.g. the powerful eathquake that happened in Japan in 2011 triggered a follow up tsunami wave [17]). This is modelled in the same way as the propagating disasters, with disaster areas having same or different epicenter and changing size and failure probability.

In Figure 2, an example of two disaster areas is given. They have different epicenter and size and might represent all three categories above, depending on whether they both occur at $t = 0$ or at different time instances. The area is plotted together with the network topology onto the same coordinate system to detect the elements of G affected by $\mathcal{D}_{k,t}$.

Our approach can capture any shape of the disaster area (uniquely defined by its geographical boundary), which allows us to define multiple and time dependent areas. We can either set an epicenter and expected radius and randomly generate the disaster area, or manually set the coordinates of the boundary of the areas. By changing the granularity of the coordinate system, the disaster area shape can be described more precisely.

Every disaster area has a failure probability assigned to it. This is the probability $p_{G,\mathcal{D}}$ of a failure of a network element in G within the area $\mathcal{D}_{x,t}$. We apply a variant of Probabilistic Region Failure Model, introduced in [18], which was originally defined on sets of concentric circles with different radius. The failure probability is monotonically decreasing with the distance from the center, and outside of the circles the failure probability drops to zero. To indicate different impact intensity (here: failure probability), (discrete) heatmaps could be applied. In the example in Figure 2, dark red reflects a high intensity impact, while the areas within the light red curve have lower intensity. The failure probability might take the distance to epicenter and the total area size into account. It can be either set as a fixed value, time-dependent probability of an area or epicenter distance-dependent within an area.

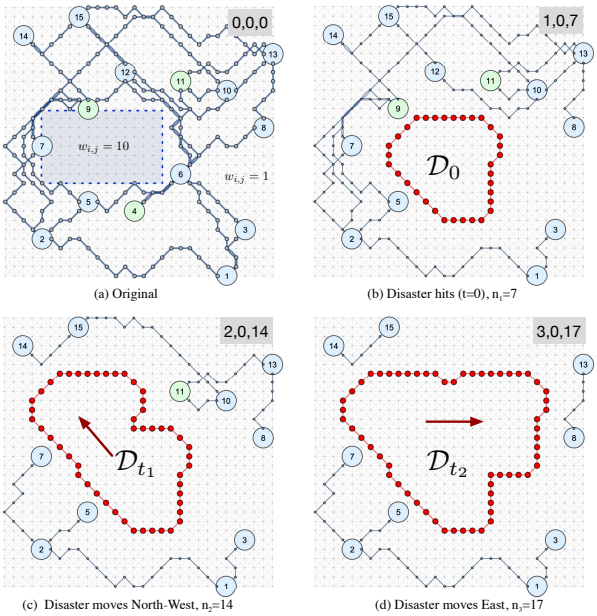

Fig. 3: Disaster is propagating over a geographical area in three stages. In the upper right corner there is a reference to the corresponding state in model in Figure 5

E. Recovery phases

In order to recover from a disastrous event, the topology (links and nodes) must be repaired. This involves both hardware repair and replacement, software restart, reboot, reload, reconfiguration and bug fixes.

In the scope of this paper, and in the example in Section V, the recovery includes rerouting of connections between peers and servers, server relocation and link/node repair. In the recovery period, multiple rerouting, relocation and repair actions will be taken, and the sequence of these actions will impact the (accumulated) performance and dependability of the system and services during recovery. In order to recommend which sequence of actions to take, we need means to assess the different alternatives.

In Section IV, algorithms are proposed for relocation and determination of the best sequence of node and link repairs. These algorithms are applied in the example in Section V.

F. Performance metrics

The metrics defined in this paper refer to the reward function applied to the (current) state x of the network topology, $M_x =$

$\mathcal{R}(G_x)$. The metrics reflect the non-functional properties of the service, i.e., the performance and dependability, and can roughly be classified in two categories.

1) *Structural metrics* - reflect the properties of the structure of the graph with respect to, for example, the relative number of peers that are connected to a server (connectivity), availability, or the number of hops in the shortest paths between each peer and the server(s). This is relevant to capture the impact of the physical network infrastructure (e.g. the optical layer).
2) *Dynamic metrics* - reflect the load dependent properties such as peer-server delay, packet losses, throughput, service reliability and availability. This is relevant to capture the influence of the packet-switched layer of the communication network.

In the example in Section V, we define $M(t)$ to be the average path length between all peers and their allocated server (according to the shortest path).

G. Survivability quantification metrics

As described in Figure 1, by considering the values of $M(t)$ over time we can obtain time dependent metrics, which will provide additional insight in how the system G evolves over time after the triggering event.

In the survivability quantification framework we discretize the phases in the recovery. A *phase* is either a stage in the disaster escalation, decay, or propagation, or a recovery action such as rerouting, relocation of servers, hardware repair, software restart or reload. The full state of the network is given by the topology graph G. A state index, or state vector, x is applied to distinguish the different network topologies, G_x. For every state x we can obtain a metric $M_x = \mathcal{R}(G_x)$. In this paper we assume that M_x is a steady state metrics, which means that network topology is (quasi-)stationary.

The next thing we need is a model where we can describe the discrete phases. Each phase corresponds to a network state G_x ($x = 1, \cdots, N_x$). Figure 4 shows an example of a survivability model, where the three disaster stages in Figure 3 are modelled. A state in this model is $x = \{i, j, k\}$, where i is the disaster stage ($i = 1, 2, 3$), j is the number of server relocations, and k is the number of remaining links to be repaired. The expected time between disasters is time $E[T_d] = 1/\mu_d$, and expected time to relocate (one, or all servers) is $E[T_r] = 1/\mu_r$. The n_1, n_2, n_3 is the number of failed links after each of the disaster stages. The models includes potential relocations of servers between the stages. A relocation will occur before the next disaster stage with probability $p_r = \mu_r/(\mu_d + \mu_r)$ (since we consider a Markov model with all time distributions being exponential). The link repairs are not shown in the figure (indicated by dotted lines to the right), see Section V and Figure 5 for the full model. In Fig. 4 you find a couple of examples of the state reward function, $M_{i,j,k}$, e.g., the metric value of the system before the disaster with no failures, $m_0 = M_{0,0,0}$, and the value immediately after the disaster, $m_a = M_{1,0,n_1}$. Observe that M_x only relies on the current state x of the network topology

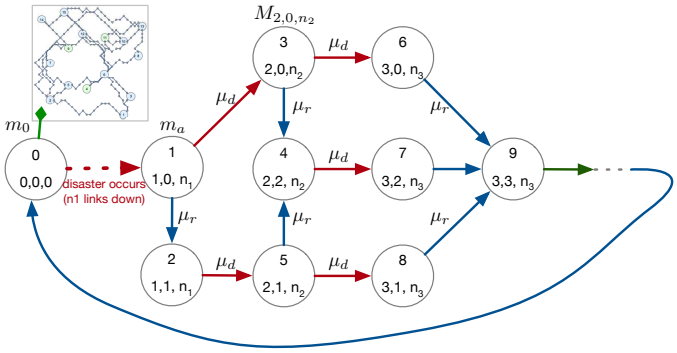

Fig. 4: Survivability model example

G_x, which is a pure structural metric. To obtain temporal metrics we need the transient probabilities from the model, $p_x(t) = p_{i,j,k}(t)$. Observe that the system is in state 1 at time $t = 0$ (immediately after the triggering event), $p_1(0) = 1$, and state 0 is an absorbing state (where the system is fully recovered, $G_0 = G$).

A time dependent metric can be obtained by:

$$M(t) = \sum_{x=0}^{N_x} p_x(t) M_x \tag{1}$$

The definitions "Survivability quantification" in Section III-A and illustrated in Figure 1, gave a few metrics that are useful to quantify both spatial and temporal properties of the system. Using $M(t)$ we may define the metrics for the consequences discussed in the introduction;

1) $m_u = M(0)$ - Instantaneous initial impact (spatial)
2) $m_a = \max_t(M(t) - m_0)$ - Maximum instantaneous impact (spatial)
3) $t_r = \{t | M(t) \leq m_r\}$ - Time until recovered to a critical level m_r (temporal)
4) $t_R = \{t | M(t) \leq m_R = m_0\}$ - Time until disaster impact has vanished and system is fully recovered (spatial and temporal);
5) $M(t) - m_0$ - Instantaneous loss (spatial (and temporal))
6) $L(t) = \int_0^t (M(u) - m_0) du$ - Accumulated loss at t (spatial and temporal);

If the assumptions related to the (quasi-)stationarity of a recovery stage and Markov properties do not hold, similar modelling approach can still be taken. The difference is that in such cases simulation should be used instead of here applied analytical approach.

H. Scalability

The scalablity of the modelling framework is determined by both the number of nodes and links of the topology (spatial dimension) and the number of disaster stages and recovery phases (time dimension).

The size of the topology (the number of nodes and links) will affect the complexity of computing the betweenness and closeness centrality of network elements. The complexity is not affected by the size, or granularity, of the underlying grid

that represents the coordinate system. This is, however, used to obtain the shortest path between the nodes (and translates to the link weights applied in the determine centrality). Hence, the calculation of the shortest path (of link segments) is affected by the granularity of the coordinate system. However, if we are studying an existing network then the link paths are already given so shortest path calculations are not necessary.

The Markov model (representing the time dimension) will grow as a function of the number of disaster stages and recovery phases since each state in the model represents a certain operational state in the network, which changes only between disaster stages and recovery phases. The size of the Markov model is therefore not directly dependent on the size of the network and the underlying coordinate system. However, the number of recovery phases depends on the number of network elements that are affected by the disaster (and the more network elements in the topology, the more elements can be affected). Furthermore, it depends on the level of details and number of stages in the description of the disaster, which might be partly dependent on the granularity in the coordinate system.

IV. Recovery strategies

An operator can undertake various actions for short-term compensation of the degradation caused by a disaster, or for long-term recovery. These actions can vary in their complexity, duration and effect, and should be tailored to the particular situation and objectives. To illustrate the capabilities of our modelling framework, we analyze three simple remediation strategies: connection rerouting, server relocation and link repair.

1) Connection rerouting: The routes between each node v and the closest server replica $s \in S$ are updated upon a disaster. The affected network topology G_x and the set of nodes hosting replicas are taken as input, while a set of routes ρ is returned as the algorithm's output. For each node v (all are peering nodes) in the network, the algorithm calculates the shortest path to each node s hosting a server replica using Dijkstra's algorithm, which considers the sum of the weights of all segments of a link as that link's weight. The closest over all servers, i.e., the one connected with a minimum-weight path, is assigned to v.

2) Server relocation: Algorithm 1 describes the process of instantiating new servers in the network affected by a disaster. The inputs to the algorithm are the network topology G_x partitioned by link cuts $\bar{E}$ into a set of connected components C, the set of nodes currently hosting a server S and the maximum number of servers S_{max} upon instantiation. The goal of the algorithm is to instantiate the available servers in the network in a way which maximizes the number of nodes that can connect to a server and minimizes the average distance to replica (i.e., the average weight of paths ρ connecting peering nodes to servers). The set of connected components is first checked to only consider those that do not contain any servers (lines 1-4), and sorted in the descending order of the component size in order to prioritize placing servers in larger components (line 5). As long as there remain unplaced replicas and connected components (lines 6-16), a server is added to the largest component (line 7). To decide which node in the component will host the server, the algorithm computes the lengths of the shortest paths connecting all other nodes in C_i and the current candidate (lines 9-13). The node with the highest closeness centrality (i.e., the lowest distance to all other nodes) is then selected to host the new server. In case there are more available servers S_{max} than connected components $|C|$, the algorithm can be extended to add servers to the components that already host replicas.

Algorithm 1: Server relocation

Data: $G_x = (V, E \setminus \bar{E})$, S, set of connected components C in the partitioned graph, number of servers to place S_{max}.
Result: The updated set S' of nodes hosting a replica

```
1  for each C_i ∈ C do
2      for each v ∈ C_i do
3          if v ∈ S then
4              C ← C \ C_i;
5  Sort set C in descending order according to the size of
     the components;
6  while S_max > 0 and |C| > 0 do
7      C_i ← C[0];
8      v_host = 0; dist_host = ∞;
9      for each v ∈ C_i do
10         dist_v = 0;
11         for each u ∈ C_i, u ≠ v do
12             ρ = Dijkstra(u, v);
13             dist_v += weight(ρ);
14         if dist_v < dist_host then
15             v_host = v; dist_host = dist_v;
16     S ← S ∪ v_host; C ← C \ C_i; S_max − −;
```

3) The sequence to repair links: We also need a procedure for determining a sequence of repairing links disrupted by a disaster. The algorithm considers the original network topology G along with the set of cut links and disconnected nodes, as well as the values of the performance metrics in the affected topology (here: average distances between peering points and the closest server α). The output of the algorithm is the repair sequence F of links deemed most beneficial. To decide on the repair sequence F, the benefit of adding each link in terms of network connectivity and average distance to the closest server is determined. The set is sorted in descending order of link centrality in an effort to evaluate the more central links first, and link checking continues until all links are repaired (alternative objective can be until all nodes are connected to a replica - or this can be an intermediate point for us to mark on the performance graph).

V. Example with a Propagating Disaster Area

Consider a network topology $G = (V, E, S)$, with $|V| = 15$ nodes, $|E| = 23$ links, $|S| = 3$ redundant servers, as shown in

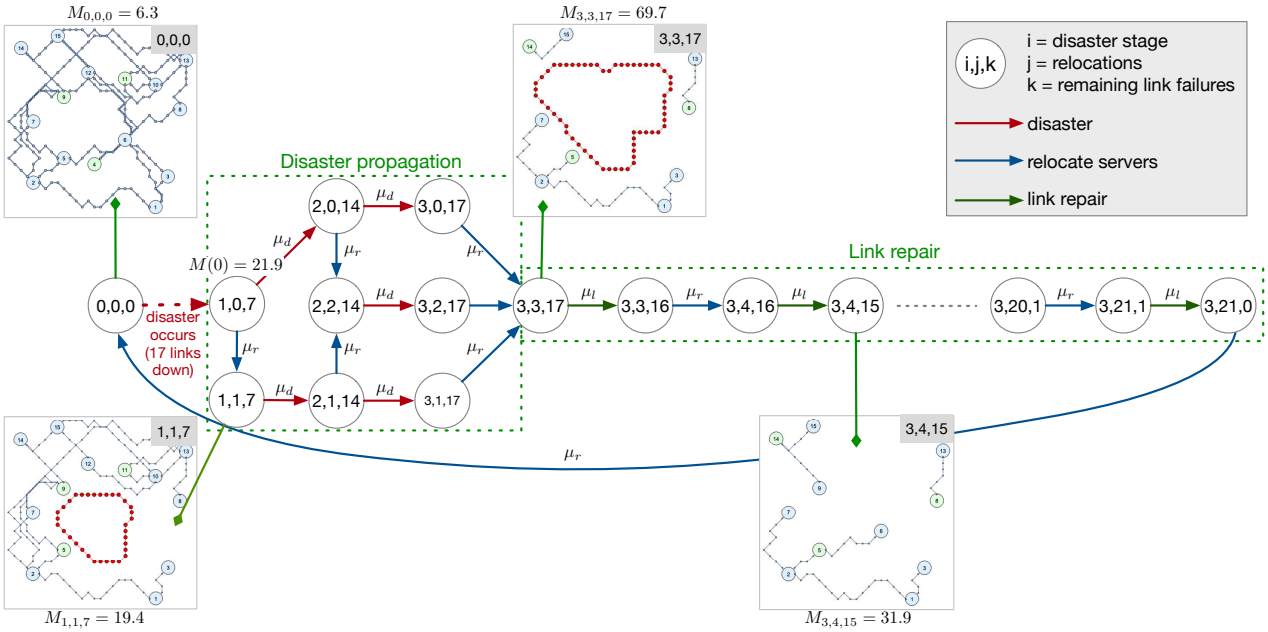

Fig. 5: The Markov model of the recovery stages for the scenario example

Figure 3(a). The weights $w_{i,j}$ in this examples are 10 within the "blue box" in the figure and 1 outside. We will demonstrate the modelling framework using a moving disaster area case scenario. This will capture both a single-hit multi-area disaster, and an escalating and propagating disaster. A propagating disaster (hurricanes/tornadoes/fire/flooding) is continuous, but for modelling purposes discretization has to be done to be able to represent the disaster propagation in a continuous time, discrete state space model (CTMC).

In this example, as illustrated in Figure 3, we consider a disaster that at $t = 0$ hits the area D_0 (Figure 3(b)), and then in the second (discretized) stage moves North-West and at t_1 covers D_{t_1} (Figure 3(c)), before it finally moves East and at t_2 covers D_{t_2} (Figure 3(d)). In this way we describe a disaster both in spatial and temporal dimensions, which is necessary to capture such a propagating disaster. The expected time between the disaster stages is $E[T_d] = 1/\mu_d$, assumed to follow a negative exponential distribution in this example. This assumption can be relaxed by using phase type distributions through semi-Markov models [19]. Alternatively, simulations with general distributions can be applied.

The probability of failure of network components within the disaster-affected areas is for simplicity set to $p_G = 1$, which means that in this example all components within the disaster area will fail. As described in Section III, this probably can be set to less than 1 to model a lower intensity of the disaster, e.g., for areas further away from the epicenter, or a disaster that gets weaker over time.

When the disaster is propagating, we assume that servers that have failed will be relocated to another node. The relocation might, or might not take place between the changes from one disaster stage to the next. In our example, the time to relocate (one, or all servers) is $T_r \sim \texttt{n.e.d.}(\mu_r)$, which means that the probability of a relocation before the next disaster stage is $\mu_r/(\mu_r + \mu_d)$. The relocation algorithm is described in Algorithm 1 in Section IV.

We assume that the expected link repair $E[T_l]$ ($T_l \sim \texttt{n.e.d.}(\mu_l)$), is much larger than time between disaster stages, and much larger than the relocation time. This implies that no link repair is completed before the disaster propagation has stopped (this can also be due to personnel safety). Between every link repair (one repair at the time), a server relocation is conducted provided that a better solution exists. The order of link repairs is defined by use of link betweenness centrality as described in Section IV.

Figure 5 contains the Markov model for the survivability quantification. The left part of the model (marked by "disaster propagation") is the model that was introduced in Figure 4, with $n_1 = 7, n_2 = 14, n_3 = 17$. This part describes the disaster propagation (Figure 3 shows the disaster stages without relocation), which captures disaster stages interchanged with (potential) relocation across the changing topology. The right part of the model (marked by dotted green and "link repair"), is an extension of Figure 4 capturing the link repair, and again interchanged with relocation, now after each link repair.

From the model in Figure 5 the metrics that were introduced in Section III-F can be obtained. To obtain the numerical values, we use the following parameters:

- Expected time between disaster stages; $E[T_d] = 1/\mu_d = 60$ [min],
- Expected time to relocate; $E[T_r] = 1/\mu_r = 3$ [min], and
- Expected link repair time; $E[T_l] = 1/\mu_l = 1000$ [min].

Figure 6 shows a plot of the $M(t)$ (Eq. (1)) over time t. The metric M used is the average path length (sum of weights on the line segments in the underlying coordinate system) of each peer-server connection (disconnected peers with infinite path

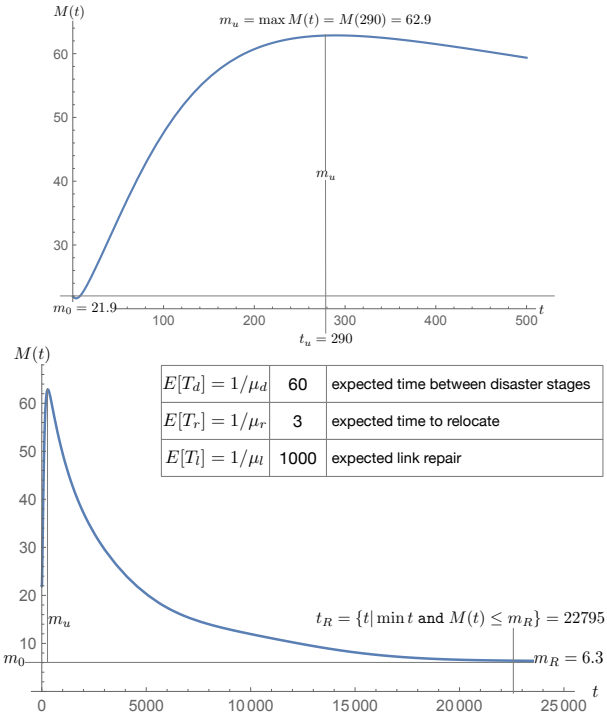

Fig. 6: The reward $R(t)$ over the disaster propagation stages and the recovery phases, in this example the reward is the average length/cost of each peer-server connections.

length, are assigned a high value of 100) in the current network topology G_x at state x. The upper figure zooms in on the first period $0 \leq t \leq 500$ after the disaster hits where the $M(t)$ is increasing (after a slight decrease when $t < 5$ (approx)), due to the propagation of the disaster with increasing impact (covering a larger area). The lower figure shows the whole period until the network is fully recovered.

In the two figures the instantaneous metric is included, $m_a = 21.9$ (spatial), as well as the maximum $m_u = 62.9$ (spatial), which occurs after $t_u = 290$ [min] (temporal), and finally the time until the system is fully recovered ($m_R = m_0$) at time $t_R = 22796$ (temporal).

Figure 7 shows the transient probabilities, $p_{3,3,17}(t)$, which is the state where the disaster has the largest extent (blue line), the $p_{r5}(t) = \sum_{\{i,j,k\} \in \mathcal{U}} p_{i,j,k}(t)$ which is the probability that 5 [out of 17] or less links have been repaired (green), and the $p_{0,0,0}(t)$ where the system is fully recovered (orange). The set $\mathcal{U}$ contains all states in the green area "Disaster propagation" in Figure 5 and the five first link repairs (out of 17).

For illustration of the usefulness of plots like the ones in Figure 7, consider the following (just three examples out of many possibilities):

1) At 17000 [min] (expected time for all link repairs) the system is fully recovered with a probability of only 0.53.
2) At 2000 [min] (expected time for 2 link repairs) the system is still in the most critical state with probability 0.13.
3) At 8000 [min] (expected time for 8 link repairs) the probability that 5 or less links have been repaired is 0.20.

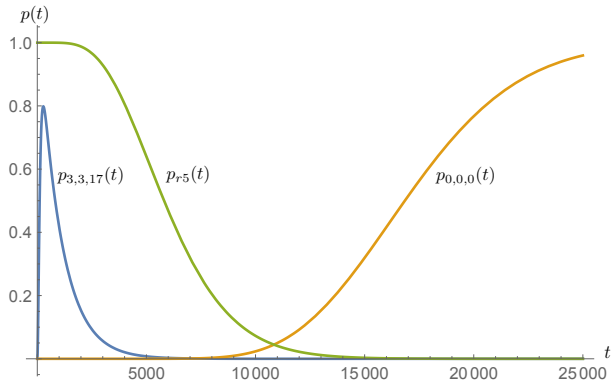

Fig. 7: Plot of the transient probabilities $p_{3,3,17}(t)$ - the state where the disaster has the largest extent, $p_{r5}(t)$ - the probability that 5 or less links have been repaired, and $p_{0,0,0}(t)$ where the system is fully recovered.

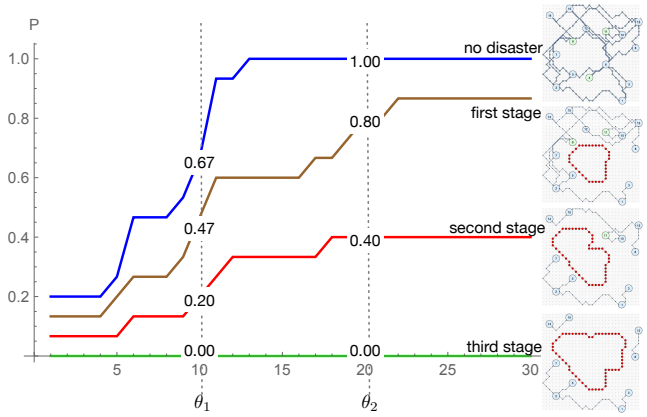

Fig. 8: The probability to be below a threshold $\theta \in [0, 30]$ for all stages in the disaster propagation given in Figure 3

The reward function of graph G_x, $M_x = \mathcal{R}(G_x)$, in this example has been the average path lengths of the peer-server pairs. An alternative is to compare every path length with a certain threshold defining the maximum "delay" tolerance (here illustrated as the path "length" where each length can be regarded as proportional to the expected delay on a link). The probability of delay below a threshold θ is estimated by the number of peer-server pairs with path length below the threshold. Peers disconnected from all servers will have an infinite path length and hence be above the threshold.

In Figure 8, the probability of propagation delay below a threshold is given for $\theta \in [0, 30]$. The figure gives specific values for $\theta_1 = 10$ and $\theta_2 = 20$ for all stages in the disaster propagation given in Figure 3. When, for instance, threshold $\theta_1 = 10$, then the reward M_x for $x = (2, 0, 14)$ (G_x in second stage) is 0.20. Changing the threshold value will change the reward for a state x although the topology of G_x is unchanged. This demonstrates the versatility of our framework in characterizing the network performance under various operator requirements. This demonstrates the versatility of our framework in characterizing the network performance under

various operator requirements. Other alternatives to M_x exists, choosing the best one depends what is the main objective of the assessment study, e.g., which criteria should be used to compare different link repair strategies.

The spatial dimension only provides insight to how many (an which) components will be affected due to a given disaster. Adding the time dimension also enables the modelling of escalating and propagating disasters, and disasters that decay and loose intensity over time. It further enables to obtain the accumulated consequence of the disaster which depends on the recovery time.

Disaster-aware network topology design can minimise/reduce the consequences in the spatial dimension, while increasing disaster preparedness (e.g., through proactive maintenance, system capacity dimensioning, competence in operation, and autonomous detection and recovery) will reduce the consequences by reducing the recovery time. To be able to assess the survivability of a system it is then crucial to include the temporal dimension as well as the spatial dimension, which is feasible with the modelling framework demonstrated in this paper.

VI. Concluding Remarks

Nowadays networks have become crucial component for vital societal needs and it is of high importance that they are reliable. A big threat to network reliability are disastrous events. Effects of natural disasters can vary over space and time - disasters can propagate, escalate or trigger a new disaster. Therefore, network recovery needs to take into account both spatial and temporal evolution of disastrous event.

In this paper, we have introduced a modelling framework for evaluation of both spatial and temporal dimensions of disaster dynamics and network multi-phased recovery actions. The framework allows for modelling of random spatial disasters areas across network topology mapped onto the same geographical coordinate system. It can capture both single-hit, propagating and escalating disaster with different intensities. No information about frequency of disaster occurrences is required since we model the transient behaviour from the time instance of the disaster occurrence (disaster is "injected").

A use case scenario with a propagating disaster was studied to show the applicability of the framework and demonstrate the importance of both spatial and temporal metrics in assessing the consequences of disaster. This provides useful insights to formulation of the best network recovery strategy from an operator's point of view. The example shows how to use the modelling framework to assess the spatial properties as the extent of a disaster area and the consequences on the network topology, as well as the temporal effects of the various recovery phases with server relocations and link repairs.

Future work will include studies of a broader set of disaster types, utilizing the obtained insights to develop optimized node and link repair as well as server relocation strategies. In addition, dynamic metrics will be considered, such as traffic load with link and server utilization, e.g., to study the impact of traffic overflow to network elements surviving a disaster. Furthermore, technical failures can still happen in the part of network topology not affected by the disaster. The combination of these failures is worth investigating because it can contribute to technical failure propagation which may lead to escalation of the consequences of the disaster. It could also be of interest to consider mapping the disaster and network topology onto a more realistic 3-dimensional coordinate system.

References

[1] P. E. Heegaard and K. S. Trivedi, "Network survivability modeling," *Comput. Netw.*, vol. 53, no. 8, pp. 1215–1234, Jun. 2009.

[2] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE T. Depend. Secure*, vol. 1, no. 1, pp. 11–33, 2004.

[3] J. Sterbenz, E. K. Çetinkaya, M. A. Hameed, A. Jabbar, S. Qian, and J. P. Rohrer, "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation," *Telecommun. Syst.*, vol. 52, pp. 705–736, 2013.

[4] J. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance," *Telecommun. Syst.*, vol. 56, pp. 17–31, 2014.

[5] L. Xie, P. E. Heegaard, and Y. Jiang, "Network survivability under disaster propagation: Modeling and analysis," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, 2013, pp. 4730–4735.

[6] J. Liu, X. Jiang, H. Nishiyama, and N. Kato, "Reliability assessment for wireless mesh networks under probabilistic region failure model," *IEEE T. Veh. Technol.*, vol. 60, no. 5, pp. 2253–2264, 2011.

[7] H. Lee, E. Modiano, and K. Lee, "Diverse routing in networks with probabilistic failures," *IEEE/ACM T. Network.*, vol. 18, no. 6, pp. 1895–1907, 2010.

[8] J. Rak, M. Pickavet, K. S. Trivedi, J. Alonso Lopez, A. M. C. A. Koster, J. P. G. Sterbenz, E. K. Cetinkaya, T. Gomes, M. Gunkel, K. Walkowiak, and D. Staessens, "Future research directions in design of reliable communication systems," *Telecommun. Syst.*, vol. 60, no. 4, p. 423–450, 2015.

[9] C. Natalino, A. Yayimli, L. Wosinska, and M. Furdek, "Infrastructure upgrade framework for content delivery networks robust to targeted attacks," *Opt. Switch. Netw.*, vol. 31, pp. 202 – 210, 2019.

[10] M. F. Habib, M. Tornatore, M. De Leenheer, F. Dikbiyik, and B. Mukherjee, "Design of disaster-resilient optical datacenter networks," *J. Lightwave Technol.*, vol. 30, no. 16, pp. 2563–2573, 2012.

[11] C. Natalino, A. de Sousa, L. Wosinska, and M. Furdek, "Content placement in 5g-enabled edge/core data center networks resilient to link cut attacks," *Networks*, vol. 75, no. 4, pp. 392–404, 2020.

[12] O. Ayoub, O. Huamani, F. Musumeci, and M. Tornatore, "Efficient online virtual machines migration for alert-based disaster resilience," in *2019 15th International Conference on the Design of Reliable Communication Networks (DRCN)*, 2019, pp. 146–153.

[13] X. Li, H. Wang, S. Yi, S. Liu, L. Zhai, and C. Jiang, "Disaster-and-evacuation-aware backup datacenter placement based on multi-objective optimization," *IEEE Access*, vol. 7, pp. 48 196–48 208, 2019.

[14] S. Ferdousi, M. Tornatore, F. Dikbiyik, C. U. Martel, S. Xu, Y. Hirota, Y. Awaji, and B. Mukherjee, "Joint progressive network and datacenter recovery after large-scale disasters," *IEEE T. Net. Serv.*, pp. 1–1, 2020.

[15] ANSI T1A1.2 Working Group on Network Survivability Performance, "Technical report on enhanced network survivability performance." ANSI, Tech. Rep. TR No. 68, February 2001.

[16] Y. Liu and K. S. Trivedi, "Survivability quantification: The analytical modeling approach," *International Journal of Performability Engineering*, vol. 2, no. 1, pp. 29–44, 2006.

[17] K. Satake and B. F. Atwater, "Long-term perspectives on giant earthquakes and tsunamis at subduction zones," *Annual Review of Earth and Planetary Sciences*, vol. 35, no. 1, pp. 349–374, 2007.

[18] J. Liu, X. Jiang, H. Nishiyama, and N. Kato, "Reliability assessment for wireless mesh networks under probabilistic region failure model," *IEEE T. Veh. Technol.*, vol. 60, no. 5, pp. 2253–2264, Jun 2011.

[19] R. A. Sahner, K. S. Trivedi, and A. Puliafito, *Performance and reliability analysis of computer system: An Example-Based Approach Using the SHARPE Software Package*. Kluwer Academic Publishers, 1996.