Telecommunication Systems

Modelling communication network challenges for Future Internet resilience, survivability, and disruption tolerance: a simulation-based approach

Egemen K. Çetinkaya · Dan Broyles · Amit Dandekar · Sripriya Srinivasan · James P. G. Sterbenz

Abstract Communication networks play a vital role in our daily lives and they have become a *critical infrastructure*. However, networks in general, and the Internet in particular face a number of challenges to normal operation, including attacks and large-scale disasters, as well as due to mobility and the characteristics of wireless communication channels. Understanding network challenges and their impact can help us to optimise existing networks and improve the design of future networks; therefore it is imperative to have a framework and methodology to study them. In this paper, we present a framework to evaluate network dependability and performability in the face of challenges. We use a simulation-based approach to analyse the effects of perturbations to normal operation of networks. We analyse Sprint logical and physical topologies, synthetically generated topologies, and present a wireless example to demonstrate a wide spectrum of challenges. This framework can simulate challenges on logical or physical topologies with realistic node coordinates using the ns-3 discrete event simulator. The framework models failures, which can be static or dynamic that can temporally and spatially evolve. We show that the impact of network challenges depends on the duration, the number of network elements in a challenge area, and the importance of the nodes in a challenge area. We also show the differences between modelling the logical router-level and physical topologies. Finally, we discuss mitigation strategies to alleviate the impact of challenges.

Keywords Internet resilience, survivability, disruption tolerance, dependability and performability, reliability and availability · ns-3 simulation · failure analysis · challenge modeling · threats and vulnerabilities · network logical and physical topology · correlated failures

E.K. Çetinkaya
E-mail: ekc@ittc.ku.edu

D. Broyles
E-mail: dbroyl01@ittc.ku.edu

A. Dandekar
E-mail: dandekar@ittc.ku.edu

S. Srinivasan
E-mail: sripriya@ittc.ku.edu

J.P.G. Sterbenz
Information and Telecommunication Technology Center,
The University of Kansas
Lawrence, Kansas, USA
and
Lancaster University,
Lancaster, UK
Tel.: +1 785 864 7890
E-mail: jpgs@{ittc.ku.edu|comp.lancs.ac.uk}

1 Introduction and Motivation

Communication networks have evolved tremendously over the past several decades, offering a multitude of services while becoming an essential critical infrastructure in our daily lives. While this evolution is still progressing, user expectations from these networks are increasing in terms of performance and dependability. On the other hand, achieving fully resilient networks is practically impossible, in part due to cost constraints, and therefore networks experience disruptions. We define *resilience* as the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation [81,80]; resilience is a discipline that subsumes survivability, fault tolerance, disruption tolerance, dependability, performability, and security.

Understanding network behaviour under perturbations can improve today's networks performance, as well as lead to a more resilient and survivable Future Internet. Therefore, it is essential to have a thorough understanding of the network behaviour when exposed to challenges, such as component failures, attacks, large-scale disasters, and effects of the mobile wireless communication environment.

Recognition of network disruptions and their causes is crucial for planning and designing networks. Some challenges to the network are inherent in the communication environment, in particular the weak and intermittent connectivity of wireless channels and dynamic topologies due to mobility. Attacks against the network are frequent, and there are also challenges caused by acts of nature such as hurricanes and solar storms. Additionally, networks are built by humans and are not completely resilient due to design flaws and cost constraints. The redundancy and diversity that increase resilience add to the cost of the network. Therefore, we need to understand the challenges and their impact on network operation and the service delivered to users.

We cannot thoroughly study the effects of challenges in live networks without impacting users. Testbeds are useful, but do not provide the scope and scale necessary to understand the resilience of large, complex networks, although progress is being made in this direction [83,75]. Simulations arguably provide the best compromise between tractability and realism to study challenges, however this is nontrivial [61].

In this paper, we present a framework to understand network behaviour when faced by challenges to communication networks. Different forms of challenges impose varying impacts, therefore they need to be modelled accordingly. Therefore, we present models to represent the various forms of challenges and show simulation results of network performance when exposed to examples of such challenges. Although we present the challenges and study the impacts on communication networks, this framework can be useful in analysis of other networks.

The rest of the paper is organised as follows: We describe challenges in communication networks and categorise them in Section 2. The evaluation methodology and implementation of challenge models are presented in Section 3. Related work is described in Section 4, followed by the simulation results in Section 5. The impact of geographically correlated failures on physical networks is presented in Section 6. We discuss challenge models and mitigation techniques in Section 7. Lastly, we summarise our findings as well as propose future work in Section 8.

2 Network Challenge Models

A *challenge* is an event that impacts normal operation of the network [81]. A *threat* is a potential challenge that might exploit a *vulnerability*. A challenge triggers *faults*, which are the hypothesized cause of *errors*. Eventually, a fault may manifest itself as an error. If the error propagates it may cause the delivered services to *fail* [7]. Challenges to the normal operation of networks include unintentional misconfiguration or operational mistakes, malicious attacks, large-scale disasters, and environmental challenges [81,82,33,31,79]. Network challenges can be categorised based on the intent, scope, and domain they impact. The network challenge taxonomy used for our simulation framework is shown in Figure 1.

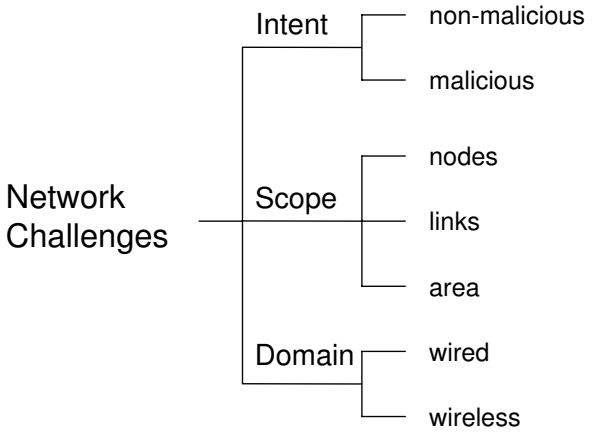


Fig. 1 Taxonomy of network challenges

It is essential to differentiate the challenges exposed and understand their impact. Next, we present the modelling of various challenges, grouped into three categories: intent, scope, and domain.

2.1 Challenge Models Based on Intent

We model the challenges based on the *intent* as malicious or non-malicious. Non-malicious challenges can be due to incompetence of an operator (e.g. accidental fiber cut, misconfiguration of network resources, large-scale outage due to power failure) or designer (e.g. hardware or software faults eventually causing a node or a link to fail). These random events affect node and link dependability, and result in the majority of the failures observed [28,45,66]. On the other hand, malicious attacks, orchestrated by an intelligent adversary, target *specific* parts of a network and can have significant impact if critical elements of the network fail. Note that while it is important to distinguish the intent in designing challenge models, the effect on network operations may be indistinguishable between malicious and non-malicious challenges.

2.2 Challenge Models Based on Scope

The *scope* of a challenge can be further categorised based on nodes, links, or network elements affected within a geographic area. While node and link failures can impact single or multiple network elements, area-based challenges usually affect multiple network elements. Natural phenomenon that are geographically correlated can impact quite large areas. Hurricanes, earthquakes, and solar storms are examples

Table 1 Examples of network challenges

Challenge Examples	Intent		Scope			Domain	
	non-malicious	malicious	nodes	links	area	wired	wireless
natural component failures [45,66]	×		×	×		×	×
misconfiguration [51,58,68]	×		×	×	×	×	×
cable cuts [72,84,69,27]	×	×		×		×	
jammers [82]		×	×	×			×
interference [82]	×			×			×
weather precipitation [38]	×			×	×		×
attack against key infrastructure components [48,71]		×	×	×		×	×
natural disasters [22,25,42,67]	×				×	×	×
pandemic [3,4]	×	×			×	×	×
nationwide Internet outage [20,21,23,24,48,69]	×	×			×	×	×
power failure [26,19]	×				×	×	×
EMP weapon [2]		×			×	×	×
coronal mass ejection [5]	×				×	×	×

of natural disasters that can impact the network at a large scale [59,67,42,5]. Malicious area-based challenges include electromagnetic pulse weapons [2]. Furthermore, geographically correlated failures can be due to dependency among critical infrastructures, as experienced in the 2003 Northeast power blackout in the US [46,26].

2.3 Challenge Models Based on Domain

Networks have quite different characteristics based on the wired or wireless domain in which they operate. Communication network performance in the wireless domain is primarily affected by the mobility of the nodes and the impairments caused by the wireless medium. The challenges that are inherent in the wireless domain include weakly, intermittently, and asymmetrically connected channels, mobility of nodes in a MANET (mobile ad-hoc network), and unpredictably long delays, particularly with store-and-forward or store-and-haul disruption tolerant networks (DTN) [82,81, 32]. These are the natural result of noise, interference, and other effects of RF propagation such as scattering and multipath, as well as the mobility of wireless nodes. Furthermore, weather events such as rain and snow can cause the signals to attenuate and impair the wireless communication network [38]. Malicious nodes may jam the signal of legitimate users to impair communication in the open wireless medium.

While the above-mentioned challenge models are orthogonal to each other, challenge scenarios are a combination of challenge sub-categories. For example, a failure due to natural aging of a component can be categorised as a non-malicious, wired (or wireless), node failure. Examples of challenges with this taxonomy are listed in Table 1.

3 Simulation Framework

In this section, we present our simulation framework to evaluate the resilience of network topologies when subject to a variety of challenges. The challenge simulation models are developed in the ns-3 [63] network simulator. Network configuration and challenge specification files are fed to our preprocessor that is the input to an ns-3 simulation.

3.1 Methodology Overview

Simulation via abstraction is one of the techniques to analyse networks in a cost-effective manner. We have chosen ns-3 [63] since it is open source, flexible, provides mixed wired and wireless capability (unlike ns-2 [62]), and the models can be extended. Unfortunately, the simulation model space increases multiplicatively with the different number of challenges and network topologies being simulated. Hence, for n different topologies subjected to c different challenges, $n \times c$ models must be generated and simulated. Our framework decouples the challenge generation from topologies by providing a comprehensive challenge specification framework, thereby reducing the simulation model space to n network $+$ c challenge models. We have created an automated simulation model generator that will combine any recognised challenge specifications with any provided topology, thus increasing the efficiency of simulation generation. Our simulation framework consists of four distinct steps as shown in Figure 2.

The first step is to provide a challenge specification that includes the type of the challenge and configuration of the challenge scenario. The second step is to provide a description of the network topology, consisting of node geographical or logical coordinates and an adjacency matrix. The third step is the automated generation of ns-3 simulation C++ code based on the topology and challenge descriptor. Finally, we run the simulations and analyse the network

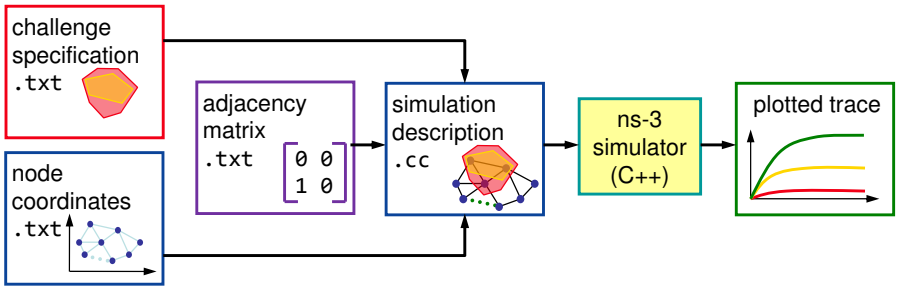


Fig. 2 Framework flow diagram

performance throughout the challenge scenario. Additionally, the simulation framework can also be enabled to generate ns-3 network animator (NetAnim) traces for visualisation purposes. A NetAnim screenshot of the Rocketfuel [77] based Sprint backbone network topology of 27 nodes and 68 links is shown in Figure 3. We have provided partial simulation code to ns-3 community that automates generation of topologies based on an adjacency matrix and node coordinates [14], which has been incorporated to the ns-3.10 standard release. Eventually, we will release the complete code base that simulates network challenges.

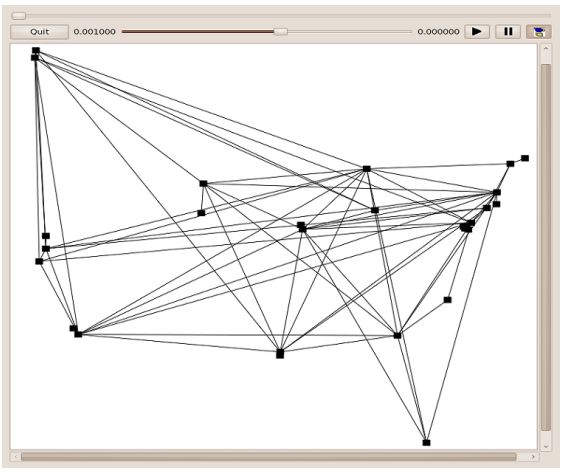


Fig. 3 NetAnim screen shot of inferred Sprint topology

3.2 Implementation of Challenge Models

In the following subsections we present the details of implementation of challenge models in the ns-3 discrete event simulator.

3.2.1 Non-malicious challenges

In the case of wired domain challenges in this category, the number of nodes or links k subject to random failure during a challenge period (t_1, t_2) is listed in the challenge specification file. Nodes or links are shut down for the duration of the challenge if the probability of failure of that node or link is greater than the probabilistic failure rate threshold p_r provided as a parameter. This type of challenge models random node and link failures that are uncorrelated with respect to topology and geography.

3.2.2 Malicious attacks

Malicious attacks result from the exploitation of structural knowledge of the network by an attacker who wishes to inflict maximum damage with limited resources. We use topological properties of the graph in order to determine the *critical* elements in the network, based on measures such as the degree of connectivity of nodes, and betweenness of nodes and links (betweenness is the number of shortest paths through a particular element [50]). The critical nodes or links are shut down for the duration of the challenge period (t_1, t_2).

3.2.3 Large-scale disasters

The challenge specification for area-based challenges resulting from large-scale disasters is an n-sided polygon with vertices located at a particular set of geographic coordinates (x_i, y_i) or a circle centered at specified coordinates (x_c, y_c) with radius r. The simulation framework then determines the nodes and links that are encompassed by the polygon or circle, and disables them during the challenge interval. We use the Computational Geometry Algorithms Library (CGAL) [1], which is an open source library with efficient geometric algorithms implemented in C++. We also implement dynamic area-based challenges, in which the challenge area can evolve in shape over time: scale (expand or contract), rotate, and move on a trajectory during the simulation. Large-scale regional failure scenarios previously only have been modelled as a static circle [8] for evaluating the performance of path restoration after a failure. Examples of the need to simulate arbitrary polygons are to model large-scale power blackouts, EMP weapons [2], coronal mass ejections [5], and large-scale natural disasters such as hurricanes and tsunami.

3.2.4 Wireless challenges

To simulate challenges in the wireless domain, we have created a new ns-3 propagation loss model that includes a mobility model parameter (e.g. random waypoint [12] or Gauss-Markov [10]) and range of influence. Using these parameters, the user can specify where the loss takes place and how it moves over time. In this way, we model a realistic challenge instead of relying solely upon statistical methods. Unlike signal loss due to scattering and line-of-sight obstacles, jammers can cause radio interference that increases channel noise and reduces the SNR (signal-to-noise ratio) that is critical to a receiver's ability to discern the data bits correctly. We implement a jammer module that sends high power signals with high data rate frames continuously on a given channel.

4 Related Work

Modelling and simulating network performance under challenge conditions is non-trivial [61]. There have been several studies that analyse different aspects of networks under challenges, however we believe this is the first unified framework that models a wide range of challenges.

Network topologies faced by random node or link failures have been studied [18, 11]. Network topologies faced by random and targeted attacks by degree of connectivity were shown to have local effect [29], since higher degree nodes that are access PoPs (Point of Presence) reside on the edge of the network. Statistical properties of logical topologies under degree-based attacks for static and dynamic evolving cases have been investigated [70,49]. Vertex and edge attacks against the wired topologies have been studied [36, 85,56,73] were based on static and dynamic topologies, in which graph metrics (degree of connectivity and betweenness) are recalculated dynamically after the attacks. Distributed denial-of-service (DDoS) attacks have been simulated using the ns-2 simulator and performance of legitimate user bandwidth is analysed for different queueing algorithms [47], but DDoS attacks generally are not targeted against infrastructure such as routers.

Internet interdomain routing performance under regional failure scenarios has been studied and found that the impact of such failures is primarily due to failure of access links in the challenge area [90]. However, this lacks a regional challenge model that can temporally and spatially evolve. Survivability of large-scale regional failures has been modelled, considering the performance of path restoration after a failure [8]. The failure scenarios consist of a regular circle centered at a point with constant radius R. In our framework the shape of failures are modelled either as a circle or as an n-sided polygon that can evolve over time.

Logical topologies can be useful to study random failures and their impacts. In our earlier work, we used logical topologies to analyse the performability of the networks under attacks [13,52]. However, physical topologies are *necessary* to study the impact of geographically correlated failures. The reliability of physical networks under disasters was studied [60,59], which presents algorithms that find a worst-case line segment and circular cut. However, disasters can take any form of shape in time and our framework can model irregular polygons dynamically.

A toolkit was previously implemented in ns-2 for simulating obstacles, however it lacks jammers and impairments [15,16].

5 Simulation Analysis

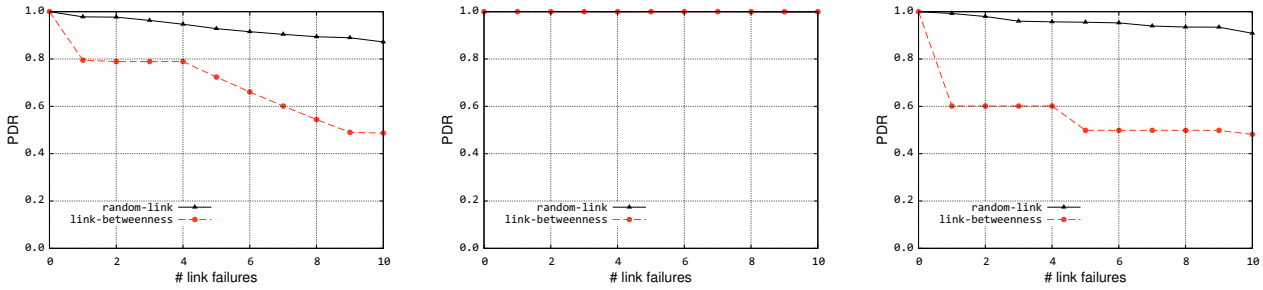
In this section, we apply our challenge framework and evaluation methodology to sample topologies to demonstrate the utility of this approach. We used ns-3.7.1 release and the simulation parameters are as follows: The network is composed of bidirectional wired links with 10 Mb/s bandwidth and 2 ms transmission delay. Routing is accomplished using the Dijkstra shortest-path-first algorithm, recalculated at each time step, with reconvergence delay as a simulation parameter. The traffic is constant bit rate (CBR) at 40 kb/s between every node pair, with 1000 Byte packets. These parameters are chosen such that there is no congestion under normal operation, but the network is not significantly overprovisioned so that we will see the effect of node and link failures. We measure the network's aggregate performance under challenges in terms of aggregate packet delivery ratio (PDR).

5.1 Non-malicious and Malicious Challenges

First, we evaluate the performance of three separate topologies shown in Figure 4 under the presence of malicious and non-malicious challenges. The topologies we choose are the Sprint topology based on the Rocketfuel map [77] (Figure 4a) and two synthetic topologies (Figure 4b and 4c). The synthetic topologies are generated using the KU-LoCGen topology generation tool [78,35,39]. KU-LoCGen generates topologies with geographic constraints and places links between nodes using various models; in this case the modified Waxman [88] model. The resulting synthetic topologies have the same number of nodes at the same geographic locations as the inferred Sprint topology, however the number of links and connectivity of the nodes differ. The two synthetic graphs chosen for this paper consist of a richly connected and poorly connected topology to demonstrate the range of robustness results from this simulation framework. The graph characteristics of three topologies are presented in Table 2.

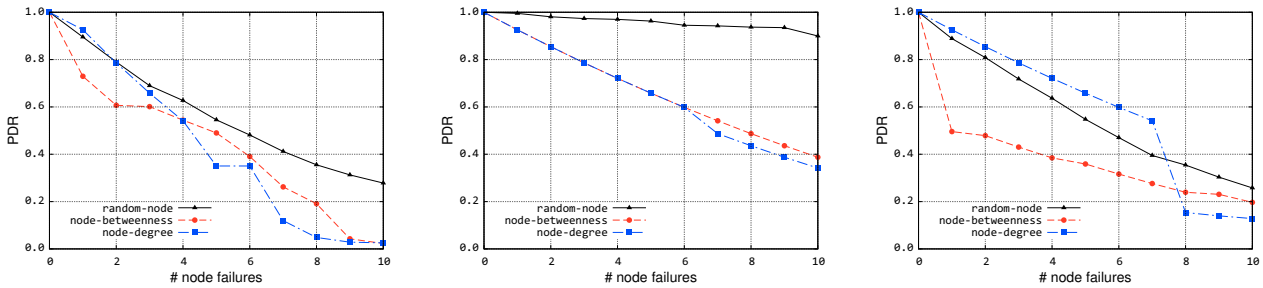
(a) Sprint inferred topology (b) Synthetic topology 1 (c) Synthetic topology 2

Fig. 4 Sample topologies for evaluation of node and link failures



(a) Sprint inferred topology (b) Synthetic topology 1 (c) Synthetic topology 2

Fig. 5 PDR during non-malicious and malicious link perturbations



(a) Sprint inferred topology (b) Synthetic topology 1 (c) Synthetic topology 2

Fig. 6 PDR during non-malicious and malicious node perturbations

Table 2 Topological characteristics of sample networks

Network Topology	Sprint	Synthetic 1	Synthetic 2
number of nodes	27	27	27
number of edges	68	74	68
maximum degree	12	9	10
average degree	5.04	5.5	5.04
clustering coeff.	0.43	0.29	0.38
network diameter	6	4	6
average hopcount	2.44	2.2	2.9
node betweenness (max/min/avg)	144/28/72	76/2/36.8	302/2/269.9
link betweenness (max/min/avg)	72/2/12.6	31/1/10.5	140/1/14.9

We evaluate the performance of the sample topologies under the presence of malicious and non-malicious challenges with the PDR of the network shown in Figure 5 for link failures and in Figure 6 for node failures with up to 10 links or nodes down. We measure the instantaneous PDR at the steady-state condition during the challenges for each point. We also note that for random failures, we average the results over 100 runs with random seed generated based on the system clock. For malicious challenges (betweenness or degree of connectivity), first we calculate the betweenness (or degree of connectivity) for each network element in the topology, and provide the challenge file as the list of the elements to be brought down in order as a function of the x-axis.

Figure 5 shows the PDR during the link perturbations to Sprint inferred (Figure 5a), synthetic 1 (Figure 5b), and synthetic 2 (Figure 5c) topologies respectively. We evaluate the PDR during link failures for two cases: 10 random link failures and an attack using the 10 highest-ranked links based on link betweenness values. Except for the synthetic topology 1, intelligent link attacks have a more degrading impact than the random failures. The PDR of 100% for both random and attack cases for the synthetic 1 topology (Figure 5b) can be attributed to this topology's lower average hop count, network diameter, clustering coefficient, and higher average degree. The synthetic topology 1 also has six more links compared to the other two topologies: 74 vs. 68. On the other hand, the link attack on highest betweenness link for synthetic topology 2 results in a PDR drop to 60%. Visual inspection of synthetic topology 2 (Figure 4c) clearly identifies the link failure between the central and west US is the cause of this since the network partitions. We can also infer the same conclusion by examining the link betweenness of synthetic topology 2 in Table 2, in which this link has 140 shortest paths.

The performance of sample topologies against malicious and non-malicious node perturbations is shown in Figure 6. We evaluate the PDR during node failures for three cases: 10 random node failures, attack of the 10 highest ranked nodes based on betweenness, and attack of the 10 highest ranked nodes based on degree of connectivity. Figures 6a, 6b, and 6c show that node failures are worse than link attacks or failures (compared to Figure 5), since each node failure is the equivalent of the failure of all links incident to that node. Our results indicate that attacks launched with knowledge of the network topology can cause the most severe degradation. We can also infer the tradeoff between robustness and the cost of building topologies using our framework. It should be noted that KU-LoCGen performs topology generation under cost constraints of a fixed and variable cost of each link, and thus we can compare the resilience of various cost points, with increasing cost providing increasing resilience due to better network connectivity when there are more links.

The performance evaluation of sample networks with varying failure probabilities is shown in Figure 7 and Figure 8. We averaged 100 simulation runs for the probabilistic failure scenarios. The seed to the random number generator is generated via the system clock, therefore we used a different seed for each run. The random variables used in the simulations were uniformly distributed. In these scenarios, PDR is calculated when the network elements are in the down state. The state transition for each element occurs if the probability of failure of a network element is greater than the specified value p_r provided in the challenge specification file.

The performance of the sample networks with increasing probabilistic node failure is shown in Figure 7. The PDR value varies between 100% and 0% as the node failure probability increases from 0% to 100%. The curves are close to each other since each sample topology has the same number of nodes, and failure probabilities are uniformly distributed. In particular, the synthetic 2 topology and Sprint inferred topologies show similar characteristics since the average degree values of those topologies are the same as listed in Table 2.

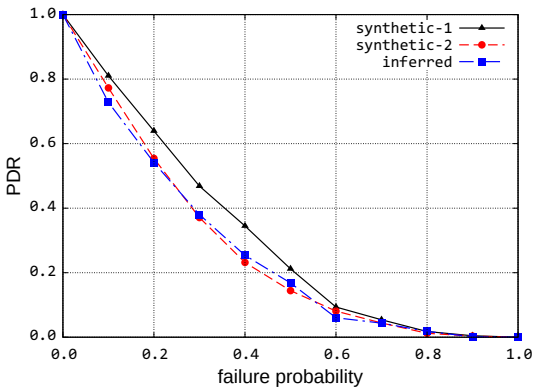


Fig. 7 Statistical node failure PDR

Figure 8 shows the PDR during the probabilistic link failures for synthetic 1, synthetic 2, and Sprint inferred topologies respectively. While the performance of the Sprint inferred and synthetic 2 topologies are close to each other, synthetic 1 topology has better performance for the probabilistic link failure scenario since it has more links compared to the other two topologies. Compared to the probabilistic node failures, probabilistic link failures do not impact the networks as much, since the impact of a node failure includes one or more links being brought down.

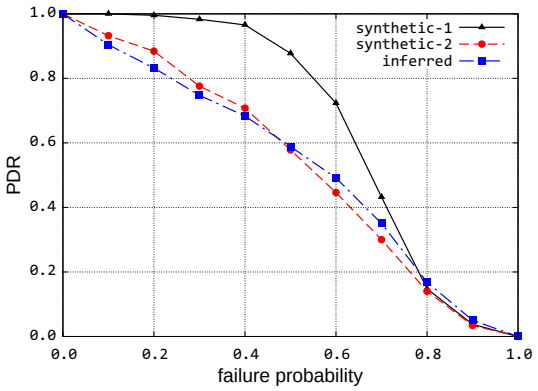
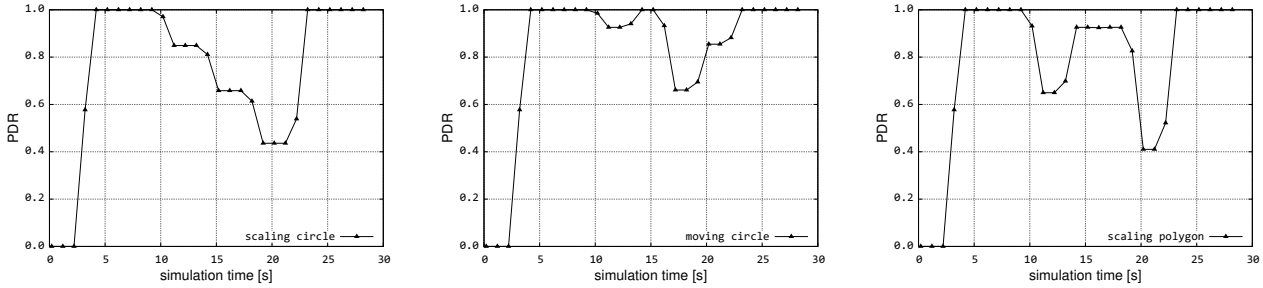


Fig. 8 Statistical link failure PDR

(a) Scaling circle (b) Moving circle (c) Scaling polygon

Fig. 9 Area-based challenge scenarios for Sprint logical topology



(a) Scaling circle PDR (b) Moving circle PDR (c) Scaling polygon PDR

Fig. 10 Area-based challenge PDR for Sprint logical topology

5.2 Area-based Challenges

As previously discussed, our framework uses circles or polygons to model geographically correlated failures representative of large-scale disasters needed to evaluate network survivability [82,30]. Area-based challenges in our model can be stationary or evolving in time. Next, we present the results of three scenarios that demonstrate area-based challenges that evolve spatially and temporally. In all scenarios, as shown in Figure 9, we use the Rocketfuel-based Sprint logical topology as shown in Figure 4a. Application traffic is generated from 2 to 29 s. and challenge scenarios were applied from 10 until 22 s for the performance plots shown in Figure 10.

5.2.1 Scaling circle

To demonstrate a scaling circle area-based challenge scenario, we simulate a circle centered at $(-74.00^\circ, 40.71^\circ)$, in New York City (NYC) as shown in Figure 9a, with a radius of 1° (approximately 111 km). We choose the scenario to be representative of an electromagnetic pulse (EMP) attack [2]. The PDR is shown in Figure 10a. We choose the simulation parameters such that the radius doubles in every 4 s. As can be seen, the PDR reduces as the circular area doubles. The PDR drop depends on how many nodes and links resides in the circle for each step.

5.2.2 Moving circle

Next, we demonstrate an area-based scenario that can evolve spatially and temporally, such as to model a hurricane. We simulate a moving circle in a trajectory from Orlando $(-81.37^\circ, 28.53^\circ)$ to NYC $(-74.00^\circ, 40.71^\circ)$. Three snapshots of the evolving challenge are shown in Figure 9b. The radius of the circle is kept at 2° (approximately 222 km). We choose the simulation parameters for illustration such that the circle reaches NYC in seven seconds (sped up to constrain simulation time), with route recomputation every 3 s.

As shown in Figure 10b, PDR reduces to 93% as the challenge starts only covering the node in Orlando at 10 s. As the challenge moves towards NYC in its trajectory, the PDR reaches one at 13 s. In this case, the challenge area includes only the link between Orlando and NYC, but since there are multiple paths, a single link failure does not affect the PDR, showing that *diversity for survivability* is crucial [81,76]. As the challenge moves into the northeast US region at 16 s., the PDR drops to 66% as the challenge covers several nodes and links. The simulation shows that as the circle moves out of the more crowded region of the network, the PDR improves, until the challenge ends at 22 s.

5.2.3 Scaling polygon

Polygons are useful to model specific geographic challenges such as power failures that can cause large-scale network

disruption as in the 2003 Northeast US blackout [26]. For a scaling polygon example, we show a 6-sided irregular polygon in the Midwest region of the US, roughly representative of the North American Electric Reliability Corporation (NERC) Midwest region [2], with vertices at: [(−87.91°, 43.04°), (−89.09°, 42.27°), (−89.64°, 39.8°), (−88.54°, 39.12°), (−88.24°, 40.12°), (−87.65°, 41.85°)] as shown in Figure 9c.

The PDR throughout the simulation is shown in Figure 10c. In this scenario, the edges of the irregular polygon increase 1.8 times every 3 s. At 10 s the challenge affects 16 links, which causes the PDR to drop to 65%. The PDR then increases to 93%, even though more links and nodes are affected at 13 s. because of route reconvergence. As the polygon increases in size, the PDR drops to as low as 41%, because the challenge area partitions the network at 21 s. This type of scenario can be used either to understand the relationship between the area of a challenge and network performability, or to model a temporally evolving challenge, such as a cascading power failure that increases in scope over time.

5.3 Wireless Domain Challenges

Wireless challenges are modelled as jammers and impairments in our ns-3 framework as discussed in Section 3. In this section, we present an example scenario that combines both types of challenges. In this scenario, a jammer node and impairment move as shown in Figure 11. The sender is located at logical coordinate (300,0), the receiver is located at (0,0), and the jammer node is located at (-100,0). During the simulation the impairment sweeps across the wireless network from left to right horizontally.

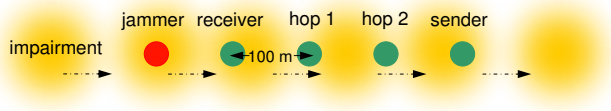


Fig. 11 Jammer and impairment combined scenario

The performance result of the above scenario is shown in Figure 12. In this scenario, the jammer is set up so that it will cause 70% packet loss for the legitimate traffic between the sender and the receiver. As the impairment sweeps horizontally, the PDR changes accordingly. In the region where the impairment affects the jammer node, 100% PDR is achieved between the sender and the receiver. As the impairment affects the receiver or sender, the PDR drops to 0%.

It should be noted that for the wireless domain challenges, a jammer's mobility pattern can cause either random or targeted attacks, depending on intentional placement near a critical node vs. a jammer with a random mobility pattern.

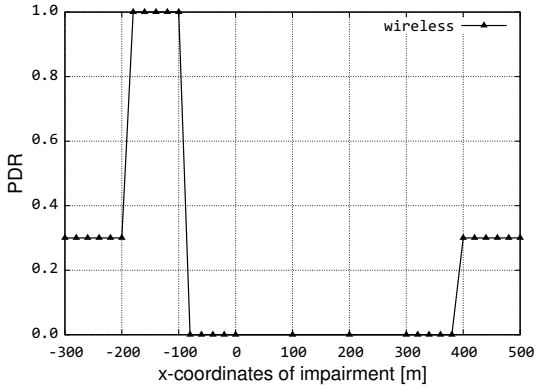


Fig. 12 Wireless challenge scenario PDR

5.4 Simulation Performance

As mentioned in Section 3, we utilised the ns-3 discrete-event simulator. Simulations that required single run were executed on a Linux based Ubuntu 9.10 computer that has a dual 1.66 GHz CPU and 1 GB RAM memory, which takes about 197 s of wall clock time to complete a single run. Execution of post processing scripts that are developed in the Perl language also takes another 166 s to strip the useful data out of the ns-3 trace files. We performed 100 run simulations on a machine with dual Intel Xeon 2.27 GHz quad-core processors with 72 GB of RAM running Linux CentOS 5.5. Each batch of 100 simulation runs, including the post-processing, took approximately 3-3.5 hours of wall clock time to complete. It should be noted that changing the packet rate and the size of topologies affects the time to complete the discrete-event simulations.

6 Impact of Challenges on Physical Topologies

Network performance analysis under a variety of challenges is possible with this framework. We showed results of how this framework can be used on a layer 3 logical topology in Section 5. In this section we investigate the network performance of a *physical layer* topology. We use the Sprint fiber-optic map shown in Figure 13[1] [43]. The map has no designation for fiber-optic nodes, instead the routes cross US cities. We project the cities to be physical node locations and connect them based on the map, which is sufficiently accurate for a national-scale map. The resulting physical topology shown in Figure 13 has 245 nodes and 287 links.

[1] Other papers [40, 17] have used this 1999 map.

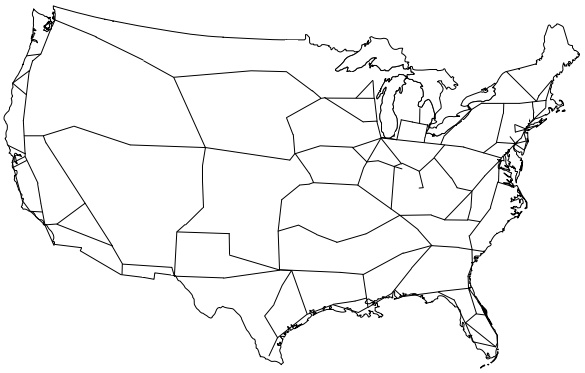


Fig. 13 Sprint fiber-optic routes

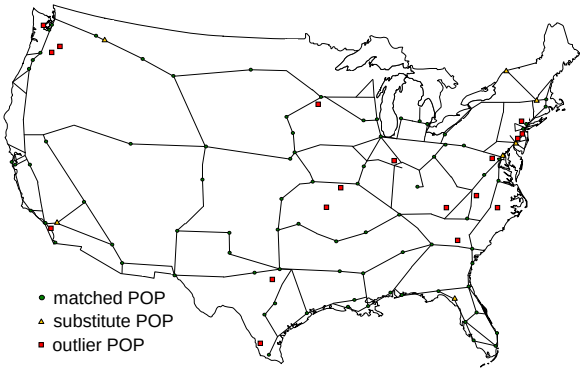


Fig. 14 Sprint MPLS PoP locations

A fiber-optic topology does not necessarily use all nodes to be traffic sources and sinks. There can be signal regenerators, cross-connects, and ADMs. Therefore, to realistically place source and sink points we utilised the Sprint global MPLS map [6], with a total of 115 MPLS PoPs in the US. Among these 115 PoPs, 83 exactly match to the physical topology we constructed. 7 more PoP locations closely match to a city on the physical topology. For example the fiber-optic route map has a point in Coeur d′Alene, Idaho, while the MPLS map has a PoP located in Post Falls, Idaho, which are very close to each other, so we consider the Coeur d′Alene node on the physical topology adjacency matrix a traffic source and sink point. 25 PoP locations did not match to the physical topology well. For example the MPLS PoP in Springfield, Missouri does not lie on any Sprint fiber routes. These MPLS PoPs are backhauled over other service providers, and are thus excluded from our Sprint traffic matrix. The resulting traffic matrix has 90 source/sink pairs. The Sprint fiber-optic routes with Sprint MPLS PoP locations are shown in Figure 14.

6.1 Challenge Simulations on Physical Topologies

The physical topology has 245 cities of which 90 MPLS PoP locations match to the cities on the physical topology. Since not all cities are traffic source or sinks, the statistical failure scenarios would not be useful determining the performability of the network. Hence, we focus on simulating area-based challenges against the physical topologies representing large-scale disasters. We run the same area-based scenarios on the physical topology that we ran on the Sprint logical topology (Section 5.2) as depicted in Figure 17.

The performance of the physical topology is shown Figure 18. The characteristics of the performance curves closely match between physical and logical topologies for the same area-based challenge scenarios. The difference is the PDR values. This is expected since the number of traffic sources and the sinks differ between each topology. We also increase the link bandwidth from 10 Mb/s to 100 Mb/s to prevent artificial drop of packets in the physical topology scenarios, since the maximum link betweenness in the physical topology is 8012 and the maximum link betweenness on the Sprint logical topology is 72.

Next, we demonstrate an area-based scenario representative of a hurricane hitting south central US as shown in Figure 15. In the smallest area are the nodes in New Orleans and Biloxi of which only the New Orleans node is a MPLS PoP node. In the second circular area challenge, the nodes are: New Orleans, Baton Rouge, Lafayette, Biloxi, and Mobile, in which 4 out of the 5 affected nodes are PoP nodes. In the largest affected area there are a total of 10 nodes, 6 of which are the PoP nodes. However, none of the three circular challenge areas cover any logical links or nodes on the map in Figure 4a, permitting us to investigate the differences between logical and physical topologies.

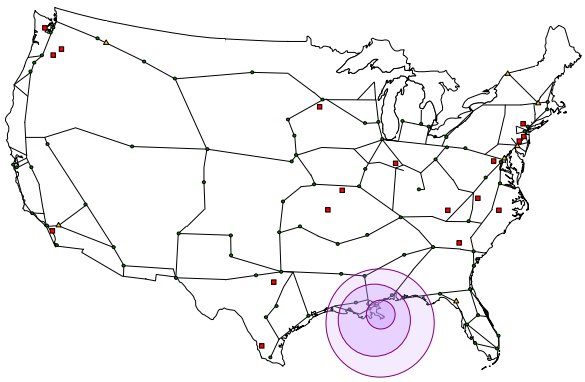


Fig. 15 South central area-based challenge scenario

The network performance of physical and logical topologies when the south central US region is challenged is shown in Figure 16. Since there are no nodes or links in the logical topology impacted, the PDR is 100%. On the other hand, the PDR of the physical topology drops to 98%, 91%, and 86%, respectively, as the challenge area covers more nodes and links. This demonstrates that it is imperative to study the impact of area-based challenges on the *physical* topologies. Traditional layer-3 logical topologies are insufficient

to understand the impact of physical challenges against the network infrastructure.

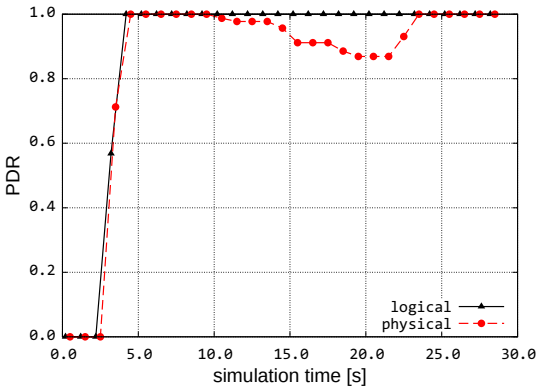


Fig. 16 South central US challenge PDR

7 Discussion

Network challenges are inherent in the communication environment. While they are inevitable [81], a thorough understanding of the consequences can help us implement proper mitigation techniques.

7.1 Network Challenges

Networks face challenges that are inherent in the environment and the consequences of these challenges can be costly. The resulting impact of these challenges is related to the probability of occurrence, the magnitude of a challenge, and the duration of a challenge. In this work we study the temporal and spatial characteristics of network challenges. Even if a challenge is an act of nature, statistical recording of such challenges can provide for the allocation of resources at the right time to reduce the impact of the challenges. Another factor contributing the probability of occurrence is social behavior: malicious attacks [89,37] affect the severity of the consequences. The magnitude of a challenge can be characterised by the following:

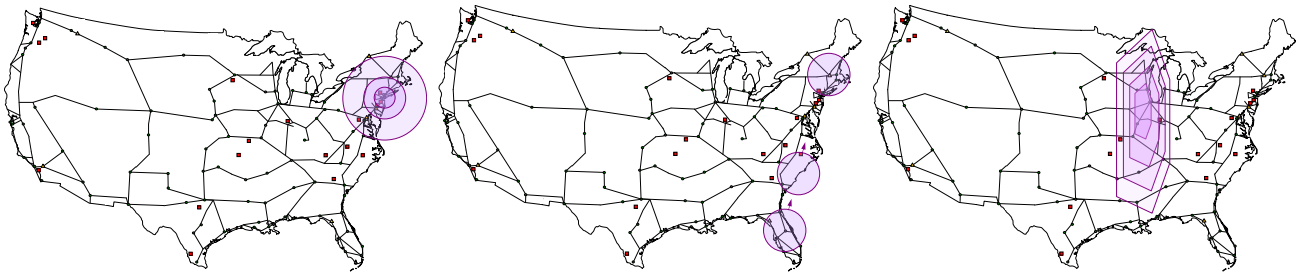
- challenge area
- number of impacted nodes and links in challenge area
- significance of network elements in the challenge area
- traffic carried through the affected area

As seen in our simulation results, magnitude of a challenge impacts the result of challenges. Finally, the duration of a challenge is critical factor impacting the network performance. This is related to the ATIS/ANSI (unservability, duration, extent) triple [86,81]. Natural or human-made disasters causing power outages increase the network downtime [71,87]. Our framework could provide valuable insight for probable consequences of network failures during the varying challenge duration. Understanding the characteristics of challenges can provide insight into the mitigation strategies to cope with various challenges.

7.2 Mitigation against Network Challenges

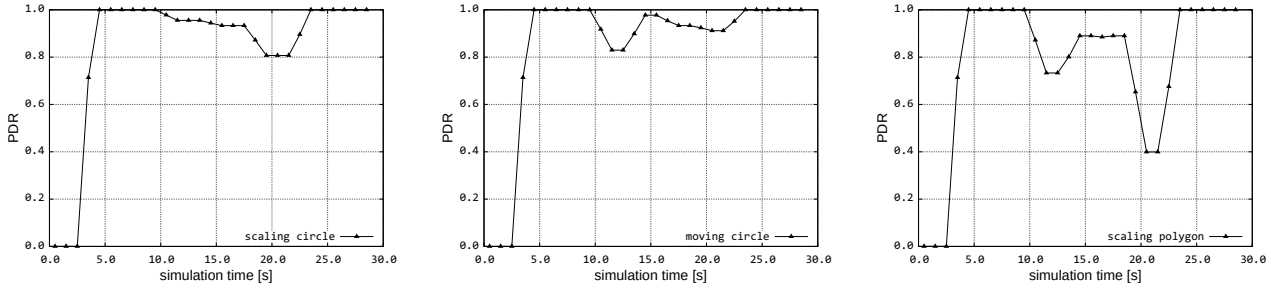
As our simulation results show, the consequence of a network challenge is degraded network state that may lead to a service impairment [81,79,78]. Since challenges exist in the communication environment inherently, we cannot avoid them, but we can mitigate the impact. So, the question to be answered is: *How to mitigate the impact of challenges?* The *enablers* for designing resilient networks are given in the ResiliNets architecture [81,80]. These enablers such as self-protection, connectivity, redundancy, diversity, and multi-level design can improve the service level of the networks, thus providing more resilient networks. Self-protection and security is necessary for the first-line of defense against attackers. Wireless networks face challenges that are inherent in the environment and DTN architectures can permit communication even when stable end-to-end paths do not exist. Redundancy can improve the service level against random failures. Spatial diversity of links between nodes resists against geographically correlated failures. Designing communication protocols and network architectures independently to improve resiliency provides multi-level aspects of resilient network design. However, these resilient network design enablers come at the cost and complexity of building these hardened systems. For example, adding new links for diverse paths or nodes for redundancy increases the total cost of the network. The challenge framework presented in this paper can be useful for design, implementation, and verification of these architectural enablers to understand how to optimally deploy components for the greatest resilience/cost ratio. This framework can also provide insight to the trade-offs of design choices.

The enablers for resilient network design are one aspect of the problem. From a policy perspective, lack of outage data hinders determining where the focus should be when designing systems. In spite of the existence of some studies that cover factors affecting the global Internet [66,68, 51,54], there is not a comprehensive study identifying the ratio of elements that contribute to the service failures in the Internet. This can be attributed to service providers' unwillingness to share outage information due to security and competitive reasons. An *open* database similar to the US FCC (Federal Communications Commission) NORS (Network Outage Reporting System) [64] for sharing outage in-



(a) Scaling circle (b) Moving circle (c) Scaling polygon

Fig. 17 Area-based challenge scenarios for Sprint physical topology



(a) Scaling circle PDR (b) Moving circle PDR (c) Scaling polygon PDR

Fig. 18 Area-based challenge PDR for Sprint physical topology

formation would benefit the research community toward increasing the resilience of the Internet.

Lastly, the human factor affects the service levels of the Internet. Approximately 50% of the PSTN failures are attributed to human related causes [45]. The situation is not any better for Internet services [34,66,58] due to misconfiguration errors caused by humans. One solution to the problem is to design better human–machine interfaces and training programs [9]. Additionally, recommended best practices can help that encompass human, management, and policy aspects for the management of telecommunication services [41].

7.3 Remediation after Network Challenges

Networks are designed based on limited resources, therefore building 100% resilient networks is not possible. The ResiliNets enablers summarised above provide guidance on *defensive* measures against network challenges. However, when networks are impacted by challenges, the enablers may be insufficient to provide the necessary service with the defenses penetrated. Therefore the effects of the challenge should be *remediated*. It should be noted that there is inconsistency in the terminology used by the community. We define remediation as to mitigate the effects of the adverse event or condition. *Recovery* involves bringing the operations to the original state [81,79,53].

This is an active area of research. Recently, *IEEE Communications Magazine* dedicated the January 2011 issue to network recovery [57,65,74,44,55]. Network recovery involves planning and preparedness, proper emergency communication, and management during a disaster.

8 Conclusions and Future Work

Recognising the challenges faced by networks is crucial for understanding network behaviour. We described how they can be categorised and presented a comprehensive framework to evaluate network performance when faced by realistic stationary or evolving challenges. This framework separates network topology from challenge specification, which increases tractability and flexibility. We demonstrated that while logical topologies are appropriate for statistical challenge scenarios or analysing network-level attacks, physical topologies are necessary to realistically study geographically correlated failures. Our results indicate that network performance varies depending on the type and severity of the challenge applied.

This paper has concentrated on illustrating the basic functionality of our challenge framework to demonstrate its utility in understanding network resilience. Future work will consist of applying this framework to a variety of real and synthetic wired, wireless, and mixed topologies to better understand the resilience of existing and future networks. Fur-

thermore, we will begin to apply this methodology to a large-scale with emulated challenges, using the GpENI (Great Plains Environment for Network Innovation) [83, 75] testbed.

Acknowledgements This is an extended version and substantial revision of a paper that appeared in IEEE/IFIP RNDM 2010 [13], with Sections 6 and 7 containing entirely new material. We would like to acknowledge Justin P. Rohrer, Abdul Jabbar, Paul Smith, Marcus Schöller, David Hutchison, and other members of the ResiliNets group for discussions on this work. We also would like to thank to Qian Shi for generating synthetic topologies and Yufei Cheng for helping to generate topology figures. We are also grateful for the helpful comments from the anonymous reviewers. This research was supported in part by NSF FIND (Future Internet Design) Program under grant CNS-0626918 (Postmodern Internet Architecture), by NSF grant CNS-1050226 (Multilayer Network Resilience Analysis and Experimentation on GENI), and by the EU FP7 FIRE Programme ResumeNet project (grant agreement no. 224619).

References

1. CGAL, Computational Geometry Algorithms Library. Http://www.cgal.org
2. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Report, Critical National Infrastructures (2004)
3. Pandemic influenza preparedness, response, and recovery guide for critical infrastructure and key resources. CI/KR guide, Department of Homeland Security (DHS) (2006)
4. Pandemic influenza impact on communications networks study. Unclassified, Department of Homeland Security (DHS) (2007)
5. Severe space weather events: Understanding societal and economic impacts. Workshop report, National Research Council (2008)
6. Sprint network maps (2010). URL `https://www.sprint.net/network_maps.php`
7. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing **1**(1), 11–33 (2004)
8. Bassiri, B., Heydari, S.S.: Network survivability in large-scale regional failure scenarios. In: Proc. of ACM C3S2E, pp. 83–87 (2009)
9. Brown, A.B.: Oops! Coping with Human Error in IT Systems. ACM Queue **2**(8), 34–41 (2004)
10. Broyles, D., Jabbar, A., Sterbenz, J.P.G.: Design and Analysis of a 3–D Gauss-Markov Mobility Model for Highly-Dynamic Airborne Networks. In: Proceedings of the International Telemetering Conference (ITC). San Diego, CA (2010)
11. Callaway, D.S., Newman, M.E.J., Strogatz, S.H., Watts, D.J.: Network Robustness and Fragility: Percolation on Random Graphs. Phys. Rev. Lett. **85**(25), 5468–5471 (2000)
12. Camp, T., Boleng, J., Davies, V.: A Survey of Models for Ad Hoc Network Research. Wireless Communication and Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends, and Applications **2**(5), 483–502 (2002)
13. Çetinkaya, E.K., Broyles, D., Dandekar, A., Srinivasan, S., Sterbenz, J.P.G.: A Comprehensive Framework to Simulate Network Attacks and Challenges. In: Proc. of the 2nd IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), pp. 538–544. Moscow, Russia (2010)
14. Çetinkaya, E.K., Jabbar, A., Broyles, D., Dandekar, A., Mahmood, R., Sterbenz, J.P.G.: Challenge modelling. `https://wiki.ittc.ku.edu/resilinets/Challenge_Modelling` (2010)
15. Chatzigiannakis, I., Kinalis, A., Mylonas, G., Nikoletseas, S., Prasinos, G., Zaroliagis, C.: TRAILS, a Toolkit for Efficient, Realistic and Evolving Models of Mobility, Faults and Obstacles in Wireless Networks. In: Proc. of 41st Annual Simulation Symposium, pp. 23–32 (2008)
16. Chatzigiannakis, I., Mylonas, G., Nikoletseas, S.: Modeling and evaluation of the effect of obstacles on the performance of wireless sensor networks. In: Proc. of 39th Annual Simulation Symposium (2006)
17. Cohen, L.: Trends in U.S. Broad-Band Fiber Optic Transmission Systems. IEEE Journal on Selected Areas in Communications **4**(4), 488–497 (1986)
18. Cohen, R., Erez, K., ben Avraham, D., Havlin, S.: Resilience of the Internet to Random Breakdowns. Phys. Rev. Lett. **85**(21), 4626–4628 (2000)
19. Cowie, J.: Lights Out in Rio. `http://www.renesys.com/blog/2009/11/lights-out-in-rio.shtml` (2009)
20. Cowie, J.: Egypt Leaves the Internet. `http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml` (2011)
21. Cowie, J.: Egypt Returns To The Internet. `http://www.renesys.com/blog/2011/02/egypt-returns-to-the-internet.shtml` (2011)
22. Cowie, J.: Japan Quake. `http://www.renesys.com/blog/2011/03/japan-quake.shtml` (2011)
23. Cowie, J.: Libyan Disconnect. `http://www.renesys.com/blog/2011/02/libyan-disconnect-1.shtml` (2011)
24. Cowie, J.: What Libya Learned from Egypt. `http://www.renesys.com/blog/2011/03/what-libya-learned-from-egypt.shtml` (2011)
25. Cowie, J., Popescu, A., Underwood, T.: Impact of Hurricane Katrina on Internet Infrastructure. report, Renesys (2005)
26. Cowie, J.H., Ogielski, A.T., Premore, B., Smith, E.A., Underwood, T.: Impact of the 2003 Blackouts on Internet Communications. Tech. rep., Renesys Corporation (2003)
27. Crawford, D.E.: Fiber Optic Cable Dig-ups: Causes and Cures. report, Network Reliability and Interoperability Council (1993)
28. Daugherty, H., Klein, W.: US network reliability issues and major outage performance. In: Proc. of ISCC, pp. 114–119 (1995)
29. Doyle, J., Alderson, D., Li, L., Low, S., Roughan, M., Shalunov, S., Tanaka, R., Willinger, W.: The "robust yet fragile" nature of the Internet. PNAS **102**(41), 14,497–14,502 (2005)
30. Ellison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff, T., Mead, N.R.: Survivable network systems: An emerging discipline. Tech. Rep. CMU/SEI-97-TR-013, Carnegie-Mellon Sorfware Engineering Institute, PA (1999)
31. ENISA Virtual Working Group on Network Providers Resilience Measures: Network resilience and security: Challenges and measures. Tech. Rep. WP 2009 – WPK 1.2 VWG 1, ENISA – European Network and Information Security Agency (2009)
32. Fall, K.: A delay-tolerant network architecture for challenged internets. In: Proc. of ACM SIGCOMM, pp. 27–34 (2003)
33. Fry, M., Fischer, M., Karaliopoulos, M., Smith, P., Hutchison, D.: Challenge identification for network resilience. In: Proc. of the IEEE 6th EURO-NF Conference on Next Generation Internet (NGI), pp. 1–8 (2010)
34. Gray, J.: A census of Tandem system availability between 1985 and 1990. IEEE Transactions on Reliability **39**(4), 409–418 (1990)
35. Hameed, M.A., Jabbar, A., Çetinkaya, E.K., Sterbenz, J.P.G.: Deriving Network Topologies from Real World Constraints. In: Proc. of IEEE GLOBECOM Workshop on Complex and Communication Networks (CCNet), pp. 415–419. Miami, FL (2010)
36. Holme, P., Kim, B.J., Yoon, C.N., Han, S.K.: Attack vulnerability of complex networks. Phys. Rev. E **65**(5), 056,109 (2002)
37. Im, G.P., Baskerville, R.L.: A longitudinal study of information system threat categories: the enduring problem of human error. ACM SIGMIS Database **36**(4), 68–79 (2005)

38. Jabbar, A., Rohrer, J., Oberthaler, A., Çetinkaya, E., Frost, V., Sterbenz, J.P.G.: Performance comparison of weather disruption-tolerant cross-layer routing algorithms. In: Proc. of IEEE INFOCOM, pp. 1143–1151 (2009)
39. Jabbar, A., Shi, Q., Çetinkaya, E., Sterbenz, J.P.G.: KU-LocGen: Location and cost-constrained network topology generator. ITTC Technical Report ITTC-FY2009-TR-45030-01, The University of Kansas, Lawrence, KS (2008)
40. Kaiser, P., Midwinter, J., Shimada, S.: Status and future trends in terrestrial optical fiber systems in North America, Europe, and Japan. IEEE Communications Magazine **25**(10), 8–13 (1987)
41. Kamoun, F.: Toward best maintenance practices in communications network management. International Journal of Network Management **15**(5), 321–334 (2005)
42. Kitamura, Y., Lee, Y., Sakiyama, R., Okamura, K.: Experience with Restoration of Asia Pacific Network Failures from Taiwan Earthquake. IEICE Trans. on Comm. **90**(11), 3095–3103 (2007)
43. KMI Corporation: North American Fiberoptic Long-haul Routes Planned and in Place (1999)
44. Krock, R.: Lack of Emergency Recovery Planning Is a Disaster Waiting to Happen. IEEE Communications Magazine **49**(1), 48–51 (2011)
45. Kuhn, D.: Sources of failure in the public switched telephone network. IEEE Computer **30**(4), 31–36 (1997)
46. Laprie, J., Kanoun, K., Kaaniche, M.: Modelling interdependencies between the electricity and information infrastructures. LNCS **4680**, 54–67 (2007)
47. Lau, F., Rubin, S., Smith, M., Trajkovic, L.: Distributed denial of service attacks. In: Proc. of IEEE SMC, vol. 3, pp. 2275–2280 (2000)
48. Lesk, M.: The New Front Line: Estonia under Cyberassault. IEEE Security and Privacy **5**(4), 76–79 (2007)
49. Magoni, D.: Tearing Down the Internet. IEEE Journal on Selected Areas in Communications **21**(6), 949–960 (2003)
50. Mahadevan, P., Krioukov, D., Fomenkov, M., Dimitropoulos, X., Claffy, K.C., Vahdat, A.: The Internet AS-level topology: three data sources and one definitive metric. ACM SIGCOMM CCR **36**(1), 17–26 (2006)
51. Mahajan, R., Wetherall, D., Anderson, T.: Understanding BGP misconfiguration. In: Proc. of the ACM SIGCOMM, pp. 3–16 (2002)
52. Mahmood, R.A.: Simulating challenges to communication networks for evaluation of resilience. Master's thesis, The University of Kansas, Lawrence, KS (2009)
53. Mannie, E., Papadimitriou, D.: Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS). RFC 4427 (Informational) (2006). URL `http://www.ietf.org/rfc/rfc4427.txt`
54. Markopoulou, A., Iannaccone, G., Bhattacharyya, S., Chuah, C.N., Ganjali, Y., Diot, C.: Characterization of Failures in an Operational IP Backbone Network. IEEE/ACM Transactions on Networking **16**(4), 749–762 (2008)
55. Mase, K.: How to Deliver Your Message from/to a Disaster Area. IEEE Communications Magazine **49**(1), 52–57 (2011)
56. Molisz, W., Rak, J.: End-to-end service survivability under attacks on networks. Journal of Telecommunications and Information Technology **3**, 19–26 (2006)
57. Morrison, K.: Rapidly Recovering from the Catastrophic Loss of a Major Telecommunications Office. IEEE Communications Magazine **49**(1), 28–35 (2011)
58. Nagaraja, K., Oliveira, F., Bianchini, R., Martin, R.P., Nguyen, T.D.: Understanding and dealing with operator mistakes in Internet services. In: Proc. of the 6th conference on Symposium on Operating Systems Design & Implementation, pp. 61–76. USENIX Association, Berkeley, CA, USA (2004)
59. Neumayer, S., Modiano, E.: Network reliability with geographically correlated failures. In: Proc. of IEEE INFOCOM, pp. 1–9 (2010)
60. Neumayer, S., Zussman, G., Cohen, R., Modiano, E.: Assessing the vulnerability of the fiber infrastructure to disasters. In: Proc. of IEEE INFOCOM, pp. 1566–1574 (2009)
61. Nicol, D., Sanders, W., Trivedi, K.: Model-based evaluation: from dependability to security. IEEE Transactions on Dependable and Secure Computing **1**(1), 48–65 (2004)
62. The ns-2 Network Simulator. `http://www.isi.edu/nsnam/ns/`
63. The ns-3 Network Simulator. `http://www.nsnam.org/`
64. US Federal Communications Commission (FCC) Network Outage Reporting System (NORS). `http://www.fcc.gov/pshs/services/cip/nors/nors.html`
65. Oberg, J., Whitt, A., Mills, R.: Disasters Will Happen – Are You Ready? IEEE Communications Magazine **49**(1), 36–42 (2011)
66. Oppenheimer, D., Ganapathi, A., Patterson, D.A.: Why Do Internet Services Fail, and What Can Be Done About It? In: Proc. of USENIX USITS, pp. 1–16 (2003)
67. O'Reilly, G., Jrad, A., Nagarajan, R., Brown, T., Conrad, S.: Critical infrastructure analysis of telecom for natural disasters. In: Proc. of IEEE Networks, pp. 1–6 (2006)
68. Pappas, V., Wessels, D., Massey, D., Lu, S., Terzis, A., Zhang, L.: Impact of configuration errors on DNS robustness. IEEE Journal on Selected Areas in Communications **27**(3), 275–290 (2009)
69. Parfitt, T.: Georgian woman cuts off web access to whole of Armenia. `http://www.guardian.co.uk/world/2011/apr/06/georgian-woman-cuts-web-access` (2011)
70. Park, S.T., Khrabrov, A., Pennock, D., Lawrence, S., Giles, C., Ungar, L.: Static and dynamic analysis of the Internet's susceptibility to faults and attacks. In: Proc. of IEEE INFOCOM, vol. 3, pp. 2144–2154 (2003)
71. Partridge, C., Barford, P., Clark, D., Donelan, S., Paxson, V., Rexford, J., Vernon, M.: The Internet Under Crisis Conditions: Learning from September 11. The National Academies Press, Washington, DC (2003)
72. Popescu, A., Premore, B., Zmijewski, E.: Impact of the Middle East Cable Breaks: A Global BGP Perspective. Presentation, Renesys Corp, San Jose, CA (2008)
73. Rak, J., Walkowiak, K.: Survivability of Anycast and Unicast Flows under Attacks on Networks. In: Proc. of the 2nd IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), pp. 497–503. Moscow, Russia (2010)
74. Ran, Y.: Considerations and Suggestions on Improvement of Communication Network Disaster Countermeasures after the Wenchuan Earthquake. IEEE Communications Magazine **49**(1), 44–47 (2011)
75. Rohrer, J.P., Çetinkaya, E.K., Sterbenz, J.P.: Progress and Challenges in Large-Scale Future Internet Experimentation using the GpENI Programmable Testbed. In: Proceedings of the 6th ACM International Conference on Future Internet Technologies (CFI), pp. 46–49. Seoul (2011)
76. Rohrer, J.P., Jabbar, A., Sterbenz, J.P.G.: Path diversification: A multipath resilience mechanism. In: Proceedings of the 7th International Workshop on the Design of Reliable Communication Networks (DRCN), pp. 343–351. Washington, DC, USA (2009)
77. Spring, N., Mahajan, R., Wetherall, D.: Measuring ISP topologies with Rocketfuel. In: Proc. of ACM SIGCOMM, pp. 133–145 (2002)
78. Sterbenz, J.P.G., Çetinkaya, E.K., Hameed, M.A., Jabbar, A., Qian, S., Rohrer, J.P.: Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation (invited paper). Telecommunication Systems (in this issue)
79. Sterbenz, J.P.G., Çetinkaya, E.K., Hameed, M.A., Jabbar, A., Rohrer, J.P.: Modelling and Analysis of Network Resilience (invited paper). In: Proc. of the 3rd IEEE/ACM International Conference on Communication Systems and Networks (COMSNETS), pp. 1–10. Bangalore (2011)

80. Sterbenz, J.P.G., Hutchison, D.: ResiliNets: Multilevel Resilient and Survivable Networking Initiative Wiki. `http://wiki.ittc.ku.edu/resilinets` (2006)
81. Sterbenz, J.P.G., Hutchison, D., Çetinkaya, E.K., Jabbar, A., Rohrer, J.P., Schöller, M., Smith, P.: Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks **54**(8), 1245–1265 (2010)
82. Sterbenz, J.P.G., Krishnan, R., Hain, R.R., Jackson, A.W., Levin, D., Ramanathan, R., Zao, J.: Survivable mobile wireless networks: issues, challenges, and research directions. In: Proc. of ACM WiSe, pp. 31–40 (2002)
83. Sterbenz, J.P.G., Medhi, D., Ramamurthy, B., Scoglio, C., Hutchison, D., Plattner, B., Anjali, T., Scott, A., Buffington, C., Monaco, G.E., Gruenbacher, D., McMullen, R., Rohrer, J.P., Sherrell, J., Angu, P., Cherukuri, R., Qian, H., Tare, N.: The Great Plains Environment for Network Innovation (GpENI): A Programmable Testbed for Future Internet Architecture Research. In: T. Magedanz, A. Gavras, N.H. Thanh, J.S. Chase (eds.) Testbeds and Research Infrastructures. Development of Networks and Communities, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 46, pp. 428–441. Springer Berlin Heidelberg (2011)
84. Styron, H.C.: CSX Tunnel Fire: Baltimore, MD. US Fire Administration Technical Report USFA-TR-140, Federal Emergency Management Administration, Emmitsburg, MD (2001)
85. Sydney, A., Scoglio, C., Youssef, M., Schumm, P.: Characterising the robustness of complex networks. International Journal of Internet Technology and Secured Transactions **2**, 291–320 (2010)
86. T1A1.2 Working Group: Network Survivability Performance. Technical Report T1A1.2/93-001R3, Alliance for Telecommunications Industry Solutions (ATIS) (1993)
87. Turner, D., Levchenko, K., Snoeren, A.C., Savage, S.: California fault lines: understanding the causes and impact of network failures. In: Proc. of the ACM SIGCOMM, pp. 315–326 (2010)
88. Waxman, B.: Routing of multipoint connections. IEEE Journal on Selected Areas in Communications **6**(9), 1617–1622 (1988)
89. Whitman, M.E.: Enemy at the gate: threats to information security. Communications of the ACM **46**(8), 91–95 (2003)
90. Wu, J., Zhang, Y., Mao, Z.M., Shin, K.G.: Internet routing resilience to failures: analysis and implications. In: Proc. of the ACM CoNEXT, pp. 1–12 (2007)

8.1 Bios*

Egemen K. Çetinkaya: is a Ph.D. candidate in the department of Electrical Engineering and Computer Science at The University of Kansas. He received the B.S. degree in Electronics Engineering from Uludağ University (Bursa, Turkey) in 1999 and the M.S. degree in Electrical Engineering from University of Missouri–Rolla in 2001. He held various positions at Sprint as a support, system, design engineer from 2001 until 2008. He is a graduate research assistant in the ResiliNets research group at the KU Information & Telecommunication Technology Center (ITTC). His research interests are in resilient networks. He is a member of the IEEE Communications Society, ACM SIGCOMM, and Sigma Xi.

Dan S. Broyles: is a Master's Degree student in the Electrical Engineering and Computer Science department at The University of Kansas. He received a Bachelor of Science degree in Electrical Engineering from Brigham Young University in 1994. He has worked in the Telecommunications industry for 16 years and is currently employed in the Technology Development organization at Sprint Nextel where he provides spectrum analysis and automation tools for other engineering teams. His interests include resilient wireless networks and backhaul strategies.

Amit Dandekar: received the M.S. degree in Information Technology from University of Kansas in 2010. He was a graduate student at the Information & Telecommunication Technology Center (ITTC). Currently Amit Dandekar works at the IBM Lenexa, Kansas lab. He has held various engineering and management positions at IBM.

Sripriya Srinivasan: is a Ph.D. candidate in the department of Electrical Engineering and Computer Science in University of Kansas. Her research interests are in resilient networks. She received B.S. degree in Instrumentation and Control Systems from University of Madras (Chennai, India) in 2000 and M.S. degree in Computer Engineering from University of Kansas in 2007. She has been employed with IBM from 2001 to present and currently working as an Advisory Software Support Engineer.

Dr. James P.G. Sterbenz: is Associate Professor of Electrical Engineering & Computer Science and on staff at the Information & Telecommunication Technology Center at The University of Kansas, and is a Visiting Professor of Computing in InfoLab 21 at Lancaster University in the UK. He received a doctorate in computer science from Washington University in St. Louis in 1991, with undergraduate degrees in electrical engineering, computer science, and economics. He is director of the ResiliNets research group at KU, PI for the NSF-funded FIND Postmodern Internet Architecture project, PI for the NSF Multilayer Network Resilience Analysis and Experimentation on GENI project, lead PI for the GpENI (Great Plains Environment for Network Innovation) international GENI and FIRE testbed, co-I in the EU-funded FIRE ResumeNet project, and PI for the US DoD-funded highly-mobile airborne networking project. He has previously held senior staff and research management positions at BBN Technologies, GTE Laboratories, and IBM Research, where he has lead DARPA- and internally-funded research in mobile, wireless, active, and high-speed networks. He has been program chair for IEEE GI, GBN, and HotI; IFIP IWSOS, PfHSN, and IWAN; and is on the editorial board of IEEE Network. He has been active in Science and Engineering Fair organisation and judging in Massachusetts and Kansas for middle and high-school students. He is principal author of the book High-Speed Networking: A Systematic Approach to High-Bandwidth Low-Latency Communication. He is a member of the IEEE, ACM, IET/IEE, and IEICE. His research interests include resilient, survivable, and disruption tolerant networking, future Internet architectures, active and programmable networks, and high-speed networking and systems.