Poster: Domino: Towards a Testbench for Stress Testing Internet Critical Infrastructure

Elham Ehsani Moghadam
ETH Zurich

Fabián E. Bustamante
Northwestern University

Adrian Perrig
ETH Zurich

Walter Willinger
NIKSUN, Inc.

***Abstract*—In just a few decades, the Internet has evolved from a research prototype to a critical infrastructure for modern society and the global economy. Despite its importance, the Internet's survivability amid large-scale failures has received limited attention. We present a testbench design for stress testing the Internet's routing system. This simulation-based framework allows for flexible integration of survivability metrics, evaluation of different topologies, and assessment of protocol and architectural changes. With several illustrative examples, we show the effectiveness of our proposed testbench and make a case for stress testing as a viable approach to evaluating the survivability of inter-domain routing against evolving challenges.**

***Index Terms*—Internet Survivability, Large-Scale Failures, Survivability Testbench, Inter-domain Routing**

I. Introduction

In just a few decades, the Internet has evolved from a research project into a critical infrastructure for the global economy and modern society, supporting other critical infrastructures such as transportation and distribution systems, the banking system, and the power grid. This evolution has been largely organic, driven by technological innovations, a changing cast of stakeholders, and emerging new applications.

Despite showing resilience against many challenges over the years, the Internet's recent designation as critical infrastructure [1] prompts the question: is it able to fulfill this role? Specifically, can it endure catastrophic events like large-scale earthquakes or prolonged power outages, cyber-attacks orchestrated by nation-states targeting its critical infrastructure systems, and extreme space weather phenomena? This concern is heightened by the Internet's central role in crisis management, enabling communication among first responders and disseminating critical information, especially in underdeveloped regions where natural disasters are becoming more frequent due to climate change.

Drawing from stress-testing methods used in critical infrastructures like the US banking system and power grid, we focus on simulating stress tests for the Internet's interdomain routing system, specifically the Border Gateway Protocol (BGP), given its critical role in global connectivity.

II. Motivation

Our work is motivated by the need to stress test the Internet's interdomain routing system against large-scale, dynamic, and prolonged failures, challenging the assumptions of existing abstract models.

979-8-3503-5171-2/24/$31.00 ©2024 IEEE

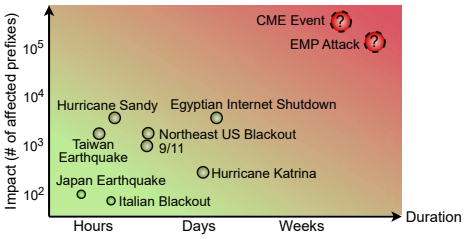

Figure 1: Failure events represented by impact and duration.

Beyond Localized Failures: The Internet has faced various resilience challenges, ranging from natural disasters to cyber-attacks. These incidents have generally been localized, affecting a limited number of prefixes for short durations. However, novel challenges posed by issues such as climate change and a growing interdependence between the Internet and the power grid introduce new vulnerabilities and the potential for widespread, prolonged failures. Additionally, extreme events like CMEs and EMP attacks, though rare, could disrupt vast regions for extended periods, highlighting the need for a deeper understanding of Internet resilience. Figure 1 contrasts the impact and duration of historical events with instances of new failure scenarios.

Beyond On/Off Failure Modes: Existing studies often simplify Internet failures as binary (on/off), but real-world scenarios are more complex, with "failing-on" conditions where network elements function intermittently or at reduced capacity. These dynamic failures are common in prolonged crises and require more attention when assessing Internet resilience.

Beyond Abstract Models: Network resilience is often studied using abstract graph models [2]. However, these models oversimplify real-world dynamics by ignoring how protocols like BGP adapt to failures.

Related Work: There is a vast body of literature on enhancing Internet resilience to attacks and natural or man-made disasters. Networking research typically focuses on physical layer [3], topology-level [4], or intra-domain [5]. Various proposals, from BGP modifications [6] to new internet architectures [7], attempt to enhance survivability, but their evaluations often lack comprehensiveness and real-world applicability.

III. Methodology and Results

We designed Domino, a testbench to evaluate the survivability of the Internet's interdomain routing system by simulating

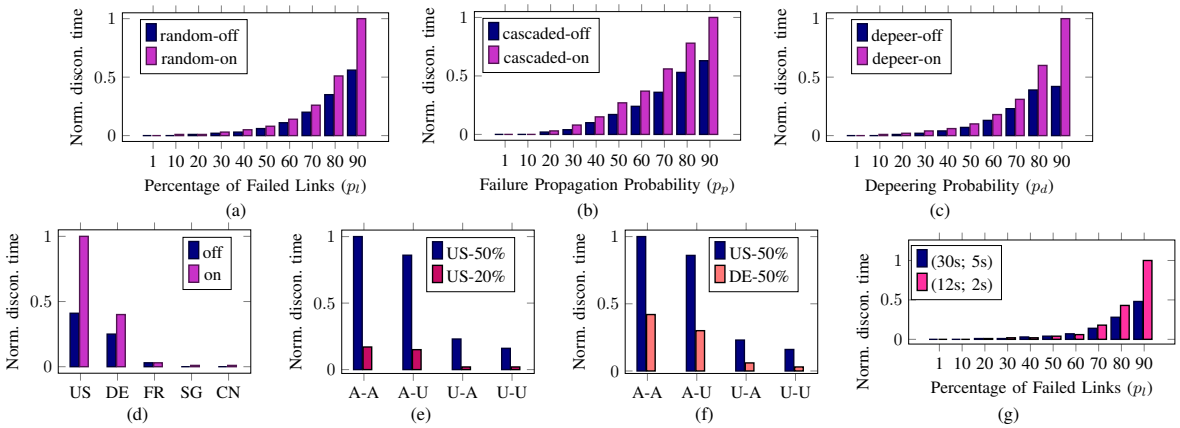

Figure 2: The impact of failure scale on disconnection time highlighting the dynamics of fail-on/fail-off for the three event scenarios: (a) random, (b) cascading, and (c) de-peering. (d) The impact of fail-on/fail-off dynamics on regional failures for different affected countries: the United States (US), Germany (DE), France (FR), Singapore (SG), and China (CN). Disconnection time for Affected-to-Affected (A-A), Affected-to-Unaffected (A-U), Unaffected-to-Affected (U-A) , and Unaffected-to-Unaffected (U-U) router-prefix pairs for (e) two failure sizes: 50% and 20% and (f) two affected regions: US and Germany. (g) The impact of the MRAI timers, for two timer pairs (eBGP; iBGP) in seconds, in the random scenario.

various failure scenarios. It simulates the impact of different failure scenarios on BGP routing and evaluates router behavior under these conditions. It then calculates a set of survivability metrics based on the simulation output.

To quantify the survivability of BGP routing, we propose an algorithm to calculate disconnection time using control plane messages. The algorithm tracks periods when a router lacks a valid path to a prefix, marking the router and its descendants as disconnected. A valid path is an available path with no loop or black hole. When a valid path is restored, the disconnection duration is recorded. This process, repeated for each update (excluding graph disconnectivity or BGP policy compliance), yields the mean disconnection time for the router-prefix pairs.

Domino supports diverse failure scenarios including regional failures affecting specific geographic areas, de-peering events where a set of AS pairs become de-peered, random failures affecting a random subset of links, and cascading failures where initial failures trigger further failures based on a propagation probability, stopping when no further failures are triggered. The fail-on approach introduces intermittent failures with a Pareto distribution to reflect real-world conditions. We use a topology with over 2,700 routers and 20,000 links across 250 ASes pruned from the CAIDA AS-rel-geo topology [8].

Figures 2a to 2d present initial stress test results for the different failure scenarios, with normalized values to highlight trends rather than absolute values. In the *Random* scenario, the x-axis shows the percentage of failed links. In the *Cascaded* scenario, it is the propagation probability—the likelihood that a neighboring link of a failed link will also fail. For the *De-peering* scenario, the x-axis shows the de-peering probability of AS pairs, while in the *Regional* scenario, it lists the affected countries. The results reveal that as failure size increases, disconnection time rises exponentially. In fail-on scenarios disconnection times are higher than in fail-off scenarios, highlighting the importance of considering failure dynamics.

Figures 2e and 2f show how disconnection time varies with failure size and location across affected and unaffected regions. Noticeable disconnection times between unaffected regions indicate insufficient failure containment.

Beyond testing different failure scenarios and regional impacts, Domino also enables the evaluation of BGP modifications. Figure 2g shows the disconnection time for two different MRAI timer values. We observe that the default MRAI timers (30s for eBGP and 5s for iBGP) prove effective in mitigating transient disconnections.

Limitations: The accuracy of publicly available Internet-wide topology and geo-location datasets, as well as the scalability of existing discrete event-driven simulators, pose well-known challenges, but using a distributed emulation environment could be one possible approach to overcome the scalability problem.

IV. Future Work

As next step, we plan to expand Domino to include additional critical infrastructure such as DNS and web infrastructure. We also plan to replace the BGP simulator with an emulator and run it at scale using a scalable architecture for the virtualization of large network scenarios.

References

[1] The European Commission, "Critical infrastructure," https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en, 2013.

[2] R. A. Barabási, H. Jeong, and Albert-László, "Error and attack tolerance of complex networks," *Nature*, no. 406, pp. 378–382, 2000.

[3] J. Rak and D. Hutchison, *Guide to disaster-resilient communication networks*. Springer Nature, 2020.

[4] J. Wu, Y. Zhang, Z. M. Mao, and K. G. Shin, "Internet routing resilience to failures: analysis and implications," in *Proceedings of the 2007 ACM CoNEXT conference*, 2007, pp. 1–12.

[5] J. P. Sterbenz, D. Hutchison *et al.*, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[6] D. Pei, X. Zhao *et al.*, "Improving BGP convergence through consistency assertions," in *Proceedings. 21st Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 2, 2002, pp. 902–911.

[7] P. B. Godfrey, I. Ganichev *et al.*, "Pathlet routing," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 4, pp. 111–122, 2009.

[8] U. CAIDA, "The CAIDA AS relationships dataset," https://www.caida.org/catalog/datasets/as-relationships/, 2022.