Internet Resilience and Survivability: Towards an Internet Architecture for the Modern World

FABIÁN E. BUSTAMANTE, Northwestern University
WALTER WILLINGER, NIKSUN, Inc.

BACKGROUND AND MOTIVATION

Over the past 50 years, the Internet has transformed from a research-focused network catering to a small group of academics into a cyber-physical infrastructure critical to modern society and the global economy. This transformation has occurred mainly by happenstance rather than design and with the underlying assumption that the architecture that has ensured the Internet's robustness in the past will be sufficient for the challenges it now faces as "critical infrastructure." However, the Internet's experience with past failure events is likely a bad predictor of its future resilience.

A quick survey of failure events the Internet has so far experienced — from man-made (e.g., cyber attacks, geo-political conflicts) to natural disasters (e.g., Tonga-like volcanic activities, Maui-like wildfires, Hurricane Ian-type wind forces and floods) — shows that past events have been single-scale in nature, with "typical" durations and sizes, lasting from less than an hour to at most a few days, and impacting anywhere from a handful of prefixes to at most a few thousands ones. In contrast, future failure events are expected to drastically differ in geographic and network scale, duration, and impact. On the one hand, climate change-induced conditions are causing natural disasters impacting ever-larger or more critical regions and lasting for extended periods, while apocalyptic events, from massive coronal mass ejections to electromagnetic pulses from high-altitude nuclear explosions and large-scale state-sponsered cyber attacks, seem no longer far-fetched. At the same time, an ever-expanding network, society's growing dependency on the applications and services built on it, and the increasing consolidation across the technology stack, have the potential to amplify the impact of failures.

Considering this radically different nature of failures and their potential impact on modern society of even a partially incapacitated Internet, it would seem unwise for our community to rely on past successes and "hope for the best."

We argue, instead, for a new research agenda that addresses the grand challenge of ensuring the Internet's resilience and survivability, and we organize this agenda around the following three high-level tasks. First, any effort to re-architect the Internet for resilience and survivability requires a new understanding of the architectural principles on which it should be based. It requires a reassessment of the possible scenarios that can threaten the network's basic functioning, as well as the threats that can arise due to the network's constant evolution, be it for economic, political, or societal reasons. Second, this re-architecting for survivability must be done in concert with the architecting of the future smart grid. This requirement arises from the observation that, among related critical cyber-physical systems, none is as interdependent with the Internet as the power grid. There cannot be a resilient Internet without a resilient power grid, and vice versa. Last, there is a critical need to develop new approaches capable of faithfully simulating the Internet at a truly global scale to, for instance, gain insights into how the current Internet behaves under different types of failure scenarios or to let us gain confidence in the viability of our designs. We next discus each of these tasks in more detail.

Authors' addresses: Fabián E. Bustamante, Northwestern University, fabianb@cs.northwestern.edu; Walter Willinger, NIKSUN, Inc., wwillinger@niksun.com.

Architectural Designs for Survivability

Tackling this ambitious research agenda starts by recognizing the new failure modes that the modern Internet faces, using them to identify architectural principles, and leveraging these principles to guide new architectural designs and developing new protocols that can ensure the network's desired robustness and survivability.

This effort could take advantage of recent progress in a theory of network architectures (i.e., layering as optimization decomposition [4]), new mathematical frameworks for scalable distributed control (i.e., system-level approach to control synthesis [1]), and attempts at the formalization of the concept of resilience engineering (i.e., understanding the behavior of designed systems when faced with "surprises" — events that were not foreseeable by the system designer [10]). For instance, such advances could be used to outline a principled approach for designing new protocols that, while ensuring that it is "business as usual" for the Internet under normal operating conditions, guarantee its survivability to multi-scale failure scenarios.

Building on a theory of network architectures, layer-specific protocols could be purposefully designed to be multi-level, implementing different closed control loops to deal with the threat models' multi-scale nature. These control loops, in turn, can be designed based on new findings that show how diversity in levels (e.g., heterogeneity in sensing, computing, and communication capabilities across levels) can be leveraged to design effective layer-specific control architectures that are fast and accurate despite the level-specific controls being slow or inaccurate (e.g., see [8]).

Specific efforts could include the design of multi-level versions of existing single-level and layer-specific Internet protocols, such as BGP and TCP, in a principled manner. They could start with attempts at quantifying the degradation in performance of traditional protocols due to inherent uncertainties in the environments in which they have to operate and examining the effects of using imperfect learning-based or statistical inference methods to enable the various closed control loops. With advances in the theory of network architecture and frameworks for distributed control, it becomes feasible to reason about Internet architectures holistically and employ such "system thinking" to analyze potential architectures for possible "surprises" and "unintended consequences" that may arise from their overall design, something that has been largely absent from systems-related networking research to date but is essential for understanding how an architecture design impacts systems performance, operation, and usage (e.g., TCP congestion collapse of 1986).

This high-level task can also complement ongoing research efforts that assume essentially a world with unlimited link bandwidth and concern the design of traffic engineering and network management methods that strive to accommodate the ever more demanding performance requirements of bandwidth-hungry and performance-sensitive next-generation applications. Unlike this 'infinite bandwidth' assumption, the 'zero bandwidth' counterpart addresses the challenges posed by survivability scenarios with very limited bandwidth in certain regions or for limited time windows. The key question is: how can we ensure basic Internet functionality in various failure scenarios? Specifically, what traffic engineering and network management techniques can be employed to make the most of the available bandwidth, regardless of its volatility, to benefit the affected population in these regions? How should any detected available bandwidth, volatile as it may be (in terms of how much bandwidth is available, where, and for how long), be used and by whom so as to best benefit the population in the impacted regions?

Designing in context - Internet and the future smart grid

The fact that among related critical cyber-physical systems, none is as interdependent with the Internet as the power grid (see also [2]), mandates that the re-architecting of the Internet for survivability must be done in close coordination with related efforts at architecting the future

power grid. In particular, as we transition from today's largely centralized power grid to one with millions of distributed and highly heterogeneous energy resources, what co-designs can ensure a future smart grid that can robustly supply the necessary power to a global-scale communication infrastructure which, in turn, is increasingly responsible for providing the very means to efficiently and securely control and manage the smart grid's operations?

The multi-scale threat models that must be considered to demonstrate the strong robustness properties expected of a modern-day Internet are also relevant for various incarnations of the future smart grid. Of particular interest in this context are threat models that account for failure events that are highly intermittent in time and space, resulting in potentially very volatile Internet connectivity or power supply, with service being available only at certain locations or time windows, perhaps as the result of attacks that leverage specific software vulnerabilities with existing, if not widely installed, patches.

On the one hand, the promise of optimally co-designing the control systems for the smart grid and the Internet hints at tantalizing opportunities for tomorrow's Internet, where smart data centers would be able to selectively and purposefully provide functionalities according to the impact of an anticipated or in-progress failure scenario. On the other hand, the efforts to transform the centralized power grid into a distributed smart grid with millions of active endpoints can also create new risks for both the smart grid and the Internet. These active endpoints are not merely passive loads (e.g., today's buildings and homes), but are also capable of generating and possibly storing energy, sensing, computing, communication, and actuation. Coordinating power supply and demand fluctuations caused by these active endpoints, especially renewable energy sources, poses significant challenges. Flaws in control system designs are likely, potentially leading to catastrophic failures resembling the 1991 telephone network outages caused by flaws in the SS7 network, an early "control plane" for the telephone network.

New approaches capable of simulating the Internet at Internet scale

Despite decade-long efforts to faithfully simulate the global Internet, Paxson & Floyd's account from some 25 years ago of "Why we don't know how to simulate the Internet" [9] is still valid today, and so is their warning that "the challenge, as always, is to reap sound insight and understanding from simulations, while never mistaking simulation for the real world" [6]. In fact, despite increasing recognition of the Internet as critical infrastructure, we still lack the basic means to simulate it in ways that let us gain insights into how the real network behaves under different types of failure scenarios or give us any confidence on the viability of our designs.

In comparison, the US Federal Reserve conducts stress tests annually "to assess whether banks are sufficiently capitalized to absorb losses during stressful conditions while meeting obligations to creditors and counterparts and continuing to be able to lend to households and businesses."[1] These stress tests involve a minimum of two different scenarios to test a bank's capital adequacy during times of stress and bank-specific results are publicly disclosed. Similarly, around 2010, there were nonpartisan studies that considered the physical security of the power grid in the US and found that while the physical destruction of just three transmission substations could cause long-term blackouts in many areas of the country, it would only require the disabling-beyond-repair of a handful of high-voltage transformers to cause a coast-to-coast blackout over an extended time.[2]

Short of using Internet "kill switch"-type approaches to induce geographically- or network-confined Internet outages such as the Egyptian government-ordered Internet shutdown of 2011[3] or

[1] https://www.federalreserve.gov/supervisionreg/stress-tests-capital-planning.htm
[2] https://crsreports.congress.gov/product/pdf/R/R43604
[3] https://www.scientificamerican.com/article/egypt-internet-mubarak/

examining accidentally caused large outages such as the Facebook outage of 2021[4] to "stress test" the Internet, we are left with no other options to study the vulnerability of the Internet as critical infrastructure than to invest renewed efforts in developing new scalable simulation engines.

These simulators have to find the right balance between being detailed enough to provide insight and understanding that can be trusted and not being too detailed so as to facilitate faithful simulations of the global Internet. By envisioning simulations of the Internet at a global scale, we are looking for analogs of the stress testing for the US banking system or the vulnerability studies of the US power grid for today's Internet. One can imagine a hybrid multiscale simulation approach [11] where the "impacted" part of the network is captured using a detailed (fine-grained) event-driven simulation involving a collection of prefixes in a geographic area or associated with a set of specific autonomous systems, where the rest of the network (the "non-impacted" part) is modeled at a coarse granularity (e.g., autonomous system-level Internet), and where the "boundary" between the two parts demands special attention to ensure a seamless coupling and information exchange between the considered two scales. Such hybrid multiscale simulations have been common in various scientific disciplines, from the material sciences to biology and the biomedical sciences, but have gained little to no traction to date in Internet research.

Related Efforts and Call for Action

We should note that the proposed agenda, while advocating for re-architecting the Internet, is not making the case for a clean-slate design. We envision, instead, alternative designs that could be deployed incrementally and let us leverage the know-how that network researchers and operators have accumulated over the years. For instance, one could imagine a particular instance of a survivable Internet architecture that builds on a resilient backbone (e.g., SCION [5] or Pathlet routing [3]) that complements the backbones relied on by large-scale service providers. This aligns well with related initiatives that advocate a new economic architecture for the Internet [7] that restructures the value and revenue chains in ways that are more effective and more incentive-driven.

Last, it should be clear by now that the success of the proposed research agenda depends critically on close collaborations among a broad and interdisciplinary team of scientists, including networking researchers, power/smart grid experts, control theorists, and economists. Only through such cross-disciplinary efforts can we expect to solve one of our community's most challenging yet important task: the re-architecting of tomorrow's Internet for resilience and survivability.

REFERENCES

[1] Anderson, J., Doyle, J., Low, S., and Matni, N. System level synthesis. *Annual Reviews in Control*, 47 (2019), 364–393.

[2] Annaswamy, A., Johansson, K., and Pappas, G. Control for societal-scale challenges: Road map 2030. *IEEE Control Systems Society Publication* (2023).

[3] Brighten, P. G., Ganichev, I., Shenker, S., and Stoica, I. Pathlet routing. *ACM SIGCOMM* (2009).

[4] Chiang, M., Low, S., Calderbank, A., and Doyle, J. Layering as optimization decomposition: A mathematical theory of network architectures. *IEEE*, 95 (2007), 255–312.

[5] Chuat, L., Legner, M., Basin, D., Hausheer, D., Hitz, S., Müller, P., and Perrig, A. *The Complete Guide to SCION. From Design Principles to Formal Verification.* Springer International Publishing AG, 2022.

[6] Floyd, S., and Paxson, V. Difficulties in simulating the internet. *IEEE/ACM Transactions on Networking 9*, 4 (2001), 392–403.

[7] Harchol, Y., Bergemann, D., Feamster, N., Friedman, E., Krishnamurthy, A., Panda, A., Ratnasamy, S., Schapira, M., and Shenker, S. A public option for the core. In *ACM SIGCOMM* (2020).

[8] Nakahira, Y., Liu, Q., Sejnowski, T., and Doyle, J. Diversity-enabled sweet spots in layered architectures and speed-accuracy trade-offs in sensorimotor control. *PNAS 118*, 22 (2021).

[9] Paxson, V., and Floyd, S. Why we don't know how to simulate the internet. In *Proc. Winter Simulation Conference* (1997).

[4] https://blog.cloudflare.com/october-2021-facebook-outage/

[10] Woods, D. Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, 141 (2015).

[11] Yang, A. On the common conceptual and computational frameworks for multiscale modeling. *Industrial & Engineering Chemistry Research*, 52 (2013), 11451–11462.