Modeling Infocommunication Networks – ELTE MSc course

Robustness of the Internet against random and deliberate attacks

Balázs Pál
Eötvös Loránd Tudományegyetem

January 14, 2021

Preliminary note

The majority of this essay was based on the 6th chapter of the book *Evolution and Structure of the Internet (A Statistical Physics Approach)* by Romualdo Pastor-Satorras. I'll reference to it just as "The book" afterwards.

1. Motivation

Since the end of the World War II, the U.S. Air Force (USAF) started to deeply analyse the circumstances of a destructive enemy attack and tried to come up with a viable plan for any possible scenario. The beginning of the Cold War further escalated this research. One of the topics included in these discussions – arisen in 1950s – was the development of a withstanding communication network, which could function even after a targeted nuclear attack (Baran, 1964).

One of the USAF's large-scale projects codenamed as *Project RAND* started in 1945 and lead by the RAND Corporation since 1948 was the one intended to connect military planning with research and development decisions in general in any field possible (Bawden, 2005). The copious amount of topics the corporation has worked on also encompassed the research of communication networks for military use and thus they also lead the development of a "survivable" network, sketched above.

Paul Baran started working on the project in 1959 and summarized the research on a network survivability in 11 memorandum in 1964, detailing the components and operation of the optimal network for the mentioned task. However the mesh-like model he proposed, later was not considered neither in the development of the ARPANET, nor in case of the Internet. Because of this, the fragility of the Internet against malfunctioning or deliberate attacks is a major issue and several practical solutions should be utilized to ensure its ordinary operation.

2. Robustness

Studies about the robustness of the Internet at the topological level have shown that in the unfortunate event of component failure, the Internet shows two very different faces to us. Against directed attacks, the resilience of the Internet is extremely low. This means that losing just a handful of nodes in key points of the network, the communication between the rest of

the nodes collapses. However in contrast, the Internet seems to be exceptionally robust against the loss of a large number of random vertices [1].

2.1. Random failures

To study the robustness of a network against either random or directed attacks, a proper and measurable, intrinsic (or in other name natural) quantity needs to be considered. The book summarizes a number of these quantities, which was efficiently used by various studies in the topic of the Internet's survivability in case of random attacks.

Independent of the chosen metric, the studies have shown, that the Internet is more fragile against small-scale attacks, than the Erdős-Rényi model, or a simple cubic mesh graph, but overwhelmingly stronger against random, large-scale failures. This behaviour can be observed both on the Internet Router (IR) and on the Autonomous System (AS) levels.

---

[1] Paul Baran. "On distributed communications networks". In: *IEEE transactions on Communications Systems* 12.1 (1964), pp. 1–9.

[2] David Bawden. "Evolution and structure of the Internet: a statistical physics approach". In: *Journal of Documentation* (2005).

[1] Notes should be made about the fact, that the book I'm using for this class was written in 2004, and the majority of its content can be considered obsolete nowadays. Since the Internet has tremendously grown in size and reached numerous technological milestones since then, this information above may not stand true in this form at the time I'm writing this essay (in early 2021).