Modelling the Internet as Spatially Constrained Interdependent Networks

Ivana Bachmann
NIC Labs, Universidad de Chile, Chile
`ivana@niclabs.cl`

Javier Bustos-Jiménez
NIC Labs, Universidad de Chile, Chile
`jbustos@niclabs.cl`

Abstract

The modern world has made the Internet a need for the people. More than ever before we have Internet dependent systems and devices. Thus, it is important to maintain the infrastructure of the Internet working properly. In order to do this first it is necessary to understand and model the behaviour of the components of the Internet network. In this paper we characterize the interactions between the Internet's physical and logical layers, and recommend a mixture of existing models from the literature to model this specific case. We study two cases of simulated Internet structures and find that an Internet physical layer embedded in a long and narrow space with Chile-like proportions of with and length is more fragile to random attacks than an Internet physical layer embedded in a square space.

1 Introduction

In our modern world communication networks are of extreme importance and the Internet is no exception. From communicating with friends to coordinating and transmitting crucial messages, the Internet is, nowadays, a big part of day to day activities in our society. Thus, we must be able to understand how the Internet works and react under conditions that may affect the Internet functionality. In particular we must understand what would happen in case of a random failure or, even worse, a targeted attack.

In order to understand what would happen to the Internet under different failure scenarios it is necessary to study its robustness. Here, we consider that Internet robustness refers to the ability of keep the users connected to the Internet in case of failure. However, to understand the Internet robustness we must also understand the underlying structures that compose it. On the one hand, there is the physical Internet network comprised by cables, antennas, routers, etc. On the other hand there is the logic Internet network comprised by autonomous systems (AS) [AS] which are connected through the BGP protocol [BGP]. These networks interact with each other allowing for the Internet to properly function. In this work we will focus on these two layers.

The area of interdependent networks studies systems composed of two or more interacting networks, with behaviours produced by such interactions that are not usually present on single networks. The study of the robustness of interdependent networks is a problem that has been explored in the last decade, leading to the development of several frameworks to tackle it. Among these frameworks we can find the "*one to one*" model presented by Buldyrev et al. [BPP+10], where they consider two interacting networks where each node depends on exactly one node in the other network with mutual dependency, this means that if a node fails then necessarily its interdependent neighbour will fail.

We can also find "*many to many*" kind of models, where each node may be interconnected to 0 or more nodes in the other network [NST13, Qiu13, DTD+14, RHB+14, CD15]. In these models dependencies may be directed or undirected. Different *many to many* models have different rules for how many node's interdependencies have to fail for the node to fail.

Other models focus more on specific characteristics of the system that want to be represented. Examples of this are the works presented in [PM13, MKT14, HLGT16] where the main purpose of the model is to represent a power grid network coupled with their control network, or the work of Li et al. [LBB+12] where main feature of the model is to represent spatially constrained networks.

In order to measure the robustness of interdependent networks different indexes and metrics are used. Some of these include the size of the giant mutually connected component [LBB$^+$12, KLCB14, ZXZX16, WKVM16], the percolation threshold [BPP$^+$10, DBBH13, LCB16], the time delay of information transmission [ZPC11], etc.

In this work we characterized the Internet as an interdependent network comprised by the physical Internet network and the logic Internet network. Here, each layer is characterized as well as the interactions between them (section 2). Using this characterization, in section 3, we provide a model and metric selected from the existing literature that can be used to study the Internet robustness considering a user based perspective of the robustness. Finally, in section 4 we simulate Internet interdependent systems and study two kinds of physical spaces: a long and narrow space with a width to length proportion of 1:25, in order to emulate the Chilean geography, and a square space with a width to length ratio of 1:1. Our finding suggests that a long and narrow geography increases the vulnerability of the Internet interdependent system.

2 Characterizing the Internet as an interdependent system

The Internet can be seen as the emerging interdependent network formed by the physical network which contains antennas, routers, cables, etc. and the logical network which contains ASs connected according to the BGP routing protocol. These networks depend on each other as each AS must be allocated on at least one working node of the physical network to stay functional, and at least one AS must be running and answering on a physical node in order for it to maintain the communication with other nodes.

In this section we characterize the Internet as an interdependent network, the physical network and the logical network are characterized in subsection 2.1 and 2.2 respectively, and the inter-dependencies between them are described in subsection 2.3.

2.1 Physical network

The physical network is the one responsible of transferring and distributing the information through physical means such as cables, optical fibers, routers, and antennas. Here, processing and redistributing information equipment such as servers, routers, or antennas correspond to the nodes of the network. While the physical means that connect the nodes, such as cables, fibers, or electromagnetic signals in the case of antennas, correspond to the links of the network.

In this network the information flow is bidirectional between each pair of nodes, thus, the links of the network are undirected links. Additionally, this network has characteristics specific to its physical nature such as distances and failure probability given their geographic location, for example, due to natural catastrophes.

Figure 1: Continental Chilean geography. The width (E-W) to length (N-S) proportion of Chile is 1:25.

2.2 logical network

The logical network is the one that maps communication routes among the ASs. An AS is a subnetwork that autonomously manages the routing within itself. On the logical network each AS represents a node while each connection given by the BGP between nodes represent a link. In this network the information flow is bidirectional, hence the links in this network are undirected. Additionally, in order for a node to have access to the Internet service it must be connected through at least one path to a Internet Service Provider (ISP), and to an International gateway to have access to the worldwide network.

2.3 Interdependencies

The physical and the logical network interact with each other, i.e., they are interdependent networks. These interactions are mutual.

On the one hand, we have that each ASs node in the logical network may be allocated in one or more nodes in the physical network. If a node in the physical network doesn't have a path to an ISP or gateway counterpart node (logical networks), then it will not have access to Internet service. As for the dependence, if all the physical nodes where a logic node is allocated fail, then the logic node will also fail, as none of its physical systems is able to communicate.

On the other hand, we have that a physical node may route a set of ASs. Hence, if all the logic nodes allocated in it fail, then the physical node won't be able to answer to any other node within the physical network, so we consider that it failed too.

This way the dependencies between networks are established as "many to many" in a bidirectional fashion, with the condition that if all of the interdependent nodes of a particular node fail, then it fails.

3 The model

Given the characterization of the interdependent system we selected from the literature a model and set of metrics. The objective was to select a framework to study the robustness of interdependent networks without mayor modifications. In order to do so we referred to the work presented in [Bac17] where 57 papers presenting or using frameworks to study the robustness on interdependent networks were reviewed.

In order to select a proper framework we considered the consumer-provider nature of the logic and the physical network. We also took into account the metric's ability to measure the users' access to the Internet.

Given the consumer-provider nature of the system as well as its "many to many" inter-dependencies, we determined that among the papers considered in [Bac17] the work presented by Parandehgheibi et al. [PM13] was the best option to analyze the case of the Internet network.

The model presented in the work of Parandehgheibi et al. consists of two networks, the Power grid network, and the Control and Communication network (CCN). Each network has provider nodes and consumer nodes. The latter nodes must have a path to a provider in order to function properly. Thus, the power grid provider has generator nodes G, and substation nodes S, while the CCN network has router nodes R, and control centers C (see figure 2).

The inter-dependencies establish support-dependence relations. This relations may be unidirectional or bidirectional. In the unidirectional case if a node in one of the networks gives support to a node in the other network, this support is not necessarily reciprocal, while in the bidirectional case it is reciprocal.

A consumer node will stay functional if there is a path from it to the a provider node and if it has at least one of their support nodes in the other network still working.

The bidirectional inter-dependencies version of this model can be directly applied over the Internet interdependent system given the characterization that we previously established (see section 2). The providers in the logical network are the nodes containing ISPs or International gateways. In the physical network the providers are the nodes where the logical network providers are allocated.

As for the physical network, its model was based on the relative neighbourhood model presented in [WKVM16] for interdependent networks, which describes the conditions to inter-connect a pair of nodes where each belong to a different physically embedded network.

We have adapted this model to build a single physical layer. In our adaptation, given a finite 2-dimensional space with a certain shape and a number of nodes N_p, each node is randomly allocated in the space. Two nodes u and v get to be connected if there is no other node in the intersection area of the circles centered at u and v, each of radius $d(v, u)$, where $d(v, u)$ is the euclidean distance between node u and v. This way, the adapted relative neighbourhood model creates a network where 2 nodes are connected if in the direction where they face each other the space is empty. This model captures a physical Internet network built with finite resources, where longer links have a higher cost relative to shorter links.

Finally, the logical network was modeled as a network with Power-law degree distribution using $\lambda = 2.7$ [FFF99] as it has been widely used to model BGP networks.

3.1 Cascading process

In the figure 2 (extracted from [PM13]) there is an example of a cascading failure process. In this example unidirectional dependencies are considered between the networks. Blue links represent support links from the CCN to the Power Grid while orange links represent support links from the Power Grid to the CCN. On step 1 S4 fails, leaving R3 without support from the Power Grid. Then, on step 2 node R3 fails. With the failure of R3, R2 has no longer a path that connects it to the control center C, also S1 and S3 loose their support from the CCN network. Thus, in step 3 R2, S1, and S3 fail. With the failure of S1, the node S2 has no longer a path to the generator node G, and the node R1 looses all support from the power grid. Hence, in step 4 R1 and S2 fail and the system reaches a total failure state.

3.2 Robustness metrics

The metric used in [PM13] is the minimum total failure removals of nodes (Node-MTFR). This metric indicates the minimum amount of nodes to be removed to cause total failure. In order to cause total failure, all the interdependent nodes must fail according to [PM13]. This characteristic allows us to measure when all the users (ASs nodes) will stop having access to the Internet as each AS is dependent on at least one physical node. Thus, this metric is useful to measure the robustness given our user oriented approach of it.

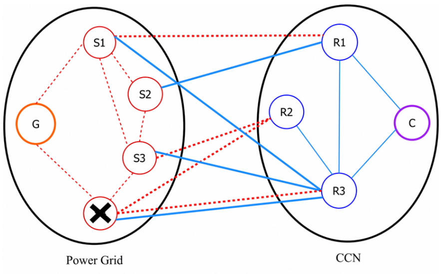
We also used the fractional size of the largest connected component in the logical network G, to measure the amount of users with Internet access, and the node-MTFR metric presented in [PM13].

4 Results

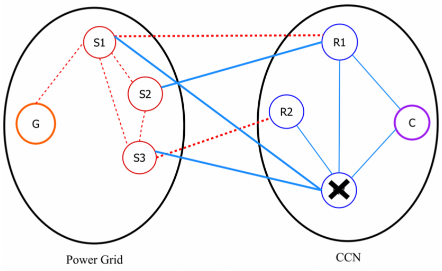
We studied the robustness of 14 simulated interdependent systems modelled according to the model presented in section 3.

Two scenarios for the physical space shape were represented, the first one representing a square space with a 1:1 width to length ratio, and the second one representing a long and narrow space such as Chile's geography (see figure 1) with a 1:25 width to length ratio. In both cases, the logical network was simulated with 300 nodes, and the physical network with 2000 nodes, following the Chilean proportions of nodes in both networks.

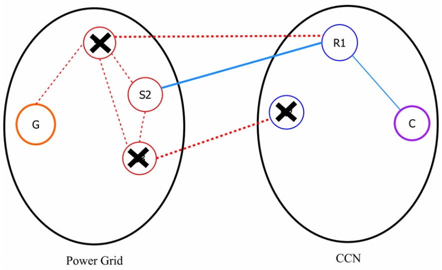
We found that G presents a continuous decay under random attacks over the whole network, meaning that no abrupt collapse is observed on the logical network under random attacks. Also, on average, the fractional size of the largest connected component of the logical network G of the system with its physical network embedded in a long and narrow space presents a faster decay in comparison to the interdependent system with its physical network embedded in a square space. We can see this result on figure 4(b), where $(1-p)$ is the fraction of nodes removed at random over the whole interdependent system. This means that less nodes have to be removed to cause the same damage to the system.



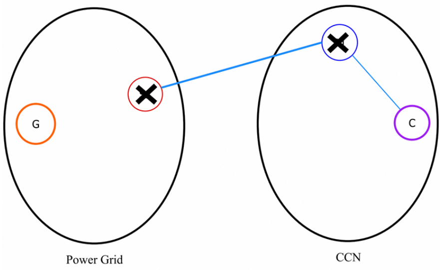
(a) Step1 - S_4 fails, initially



(b) Step2 - R_3 fails



(c) Step3 - S_1, S_3 and R_2 fail



(d) Step4 - R_1 and S_2 fail

Figure 2: Cascading process as presented in [PM13].

We also observed that the node-MTFR of both systems remain really close to the total amount of nodes in the logical network (see table 1), which is less than the average amount of nodes that must be removed under random attacks to cause the same damage.

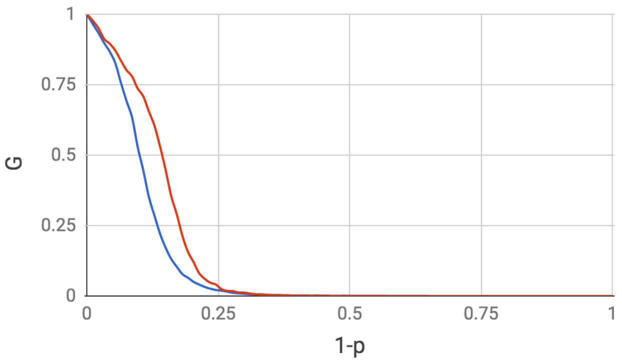


Figure 3: Results for long and narrow physical space averages on the left, and square space averages on the right.

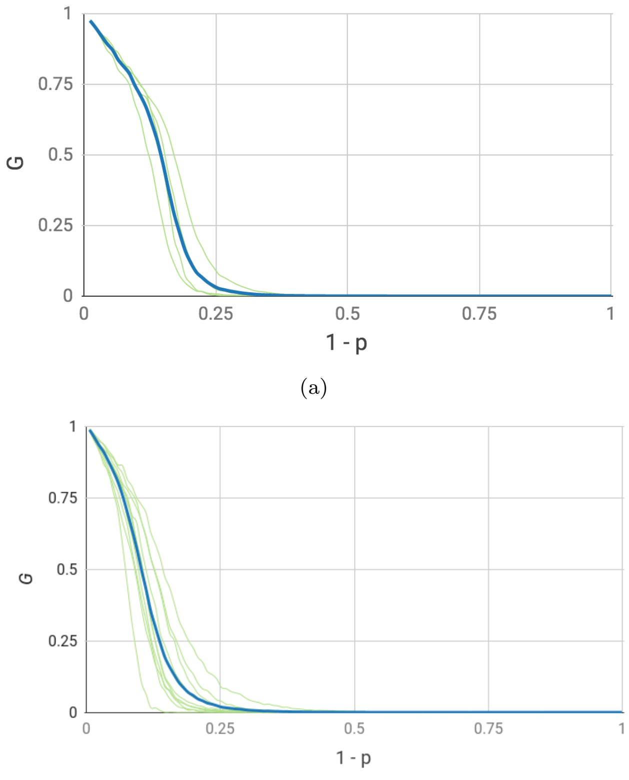
Table 1: Average node-MTFR by space type

Space type	mean node-MTFR
Long and narrow	299.9
Square	299.25

4.1 Square physical space

For the square physical space 4 interdependent systems were simulated. Each system was randomly attacked to study their robustness, and for each system the node-MTFR was calculated. In figure 4(a) we show the average results obtained over 100 iterations of the random attacks. In table 1 we show the average node-MTFR for these simulated interdependent networks.

Similar to the case of a long and narrow physical space it can be seen that node-MTFR is able to cause total failure by removing about 13% of the system's nodes (299 nodes out of 2300, see Table 1), while under random attacks 30% of the nodes must be removed for G to be under 0.01.



(a)

(b)

Figure 4: Green lines show each simulation results. Blue line shows average of all simulations. In (a) Results for square physical space. In (b) Results for long and narrow physical space.

4.2 Long and narrow physical space

The long and narrow physical space follows the Chilean country width to length proportion of 1:25. An image of the country can be seen in figure 1. For the physical space 10 interdependent systems were simulated. Each system was randomly attacked to study their robustness, and for each system the node-MTFR was calculated. In figure 4(b) we show the average results obtained over 100 iterations of the random attacks, and in table 1 the average node-MTFR value obtained for each pair of networks is simulated. We can observe that under random attacks about 29% of nodes must be removed of the interdependent system in order to reach values of G inferior to 0.01, while node-MTFR can cause total failure by removing only 13% of the nodes in the system.

5 Conclusions

In this work we characterized the Internet as the interdependent system comprised by the Internet logical network and the Internet physical network. We found a model and a metric suitable for studying the Internet from the literature 'as is', and we used it over simulated physical and logical networks. It was also proposed a modified version of the relative neighborhood model presented in [WKVM16] to simulate physical networks. Using this modified relative neighborhood model we randomly attacked 2 types of systems. One with its physical network embedded in a square space, and another with its physical network embedded in a long and narrow space following the proportions of Chile. We found that the narrow and long space physical networks results in a more fragile interdependent system structure from the user's point of view. This suggests that studying the particular scenarios of countries with geographies similar to the Chilean one may be of special concern when studying Internet robustness. Finally, we observed that node-MTFR may be a more accurate measure of Internet infrastructure robustness than random attack as less nodes are required to cause total failure in comparison to random attacks. As future work remains to study the effect on the robustness of randomly attacking each network separately, as well as studying different coupling patterns of the interacting networks, different amount of providers, and space configurations for the Internet physical network. It is of special interest for the case of the Chilean Internet to analyze the effect of physical networks that contain areas where nodes can't be placed on. This areas could be used to represent geographic features such as islands or mountains which are prevalent on the Chilean geography.

Acknowledgement

This work was partially funded by CONICYT Doctorado Nacional 21170165.

References

[AS] Autonomous system. `https://tools.ietf.org/html/rfc1930`. Accessed: 03-07-2017.

[Bac17] Ivana Bachmann. Framework de estudio multi-capa para resiliencia de Internet chileno. Master's thesis, Universidad de Chile, Santiago, Chile, 2017.

[BGP] Border gateway protocol. `https://tools.ietf.org/html/rfc4271`. Accessed: 03-07-2017.

[BPP+10] Sergey V Buldyrev, Roni Parshani, Gerald Paul, H Eugene Stanley, and Shlomo Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025–1028, 2010.

[CD15] Srinjoy Chattopadhyay and Huaiyu Dai. Towards optimal link patterns for robustness of interdependent networks against cascading failures. In *2015 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2015.

[DBBH13] Michael M Danziger, Amir Bashan, Yehiel Berezin, and Shlomo Havlin. Interdependent spatially embedded networks: dynamics at percolation threshold. In *Signal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on*, pages 619–625. IEEE, 2013.

[DTD+14] Gaogao Dong, Lixin Tian, Ruijin Du, Min Fu, and H Eugene Stanley. Analysis of percolation behaviors of clustered networks with partial support–dependence relations. *Physica A: Statistical Mechanics and its Applications*, 394:370–378, 2014.

[FFF99] Michalis Faloutsos, Petros Faloutsos, and Christos Faloutsos. On power-law relationships of the internet topology. In *ACM SIGCOMM computer communication review*, volume 29, pages 251–262. ACM, 1999.

[HLGT16] Yuqi Han, Zhi Li, Chuangxin Guo, and Yuezhong Tang. Improved percolation theory incorporating power flow analysis to model cascading failures in cyber-physical power system. In *Power and Energy Society General Meeting (PESGM), 2016*, pages 1–5. IEEE, 2016.

[KLCB14] Yosef Kornbluth, Steven Lowinger, Gabriel Cwilich, and Sergey V Buldyrev. Cascading failures in networks with proximate dependent nodes. *Physical Review E*, 89(3):032808, 2014.

[LBB+12] Wei Li, Amir Bashan, Sergey V Buldyrev, H Eugene Stanley, and Shlomo Havlin. Cascading failures in interdependent lattice networks: The critical role of the length of dependency links. *Physical review letters*, 108(22):228702, 2012.

[LCB16] Steven Lowinger, Gabriel A Cwilich, and Sergey V Buldyrev. Interdependent lattice networks in high dimensions. *Physical Review E*, 94(5):052306, 2016.

[MKT14] Yuki Matsui, Hideharu Kojima, and Tatsuhiro Tsuchiya. Modeling the interaction of power line and scada networks. In *2014 IEEE 15th International Symposium on High-Assurance Systems Engineering*, pages 261–262. IEEE, 2014.

[NST13] Duy T Nguyen, Yilin Shen, and My T Thai. Detecting critical nodes in interdependent power networks for vulnerability assessment. *Smart Grid, IEEE Transactions on*, 4(1):151–159, 2013.

[PM13] Marzieh Parandehgheibi and Eytan Modiano. Robustness of interdependent networks: The case of communication networks and the power grid. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 2164–2169. IEEE, 2013.

[Qiu13] Yuzhuo Qiu. The effect of clustering-based and degree-based weighting on robustness in symmetrically coupled heterogeneous interdependent networks. In *2013 IEEE International Conference on Systems, Man, and Cybernetics*, pages 3984–3988. IEEE, 2013.

[RHB+14] Saulo DS Reis, Yanqing Hu, Andrés Babino, José S Andrade Jr, Santiago Canals, Mariano Sigman, and Hernán A Makse. Avoiding catastrophic failure in correlated networks of networks. *Nature Physics*, 10(10):762–767, 2014.

[WKVM16] Xiangrong Wang, Robert E Kooij, and Piet Van Mieghem. Modeling region-based interconnection for interdependent networks. *Physical Review E*, 94(4):042315, 2016.

[ZPC11] Xian Zhang, Chris Phillips, and Xiuzhong Chen. An overlay mapping model for achieving enhanced qos and resilience performance. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on*, pages 1–7. IEEE, 2011.

[ZXZX16] Xue-Jun Zhang, Guo-Qiang Xu, Yan-Bo Zhu, and Yong-Xiang Xia. Cascade-robustness optimization of coupling preference in interconnected networks. *Chaos, Solitons & Fractals*, 92:123–129, 2016.