Universitat de Girona

NEW ROBUSTNESS EVALUATION MECHANISMS FOR COMPLEX NETWORKS

Marcos MANZANO CASTRO

Dipòsit legal: Gi. 646-2015
http://hdl.handle.net/10803/295713

DOCTORAL THESIS

NEW ROBUSTNESS EVALUATION MECHANISMS FOR COMPLEX NETWORKS

Marcos Manzano Castro

2014

DOCTORAL THESIS

NEW ROBUSTNESS EVALUATION MECHANISMS FOR COMPLEX NETWORKS

Marcos Manzano Castro

2014

Ph.D. TECHNOLOGY PROGRAM

Advisor: Dr. Eusebi Calle

Submitted in fulfillment of the requirements
of the degree of PhD by the University of Girona

When someone seeks," said Siddhartha, "then it easily happens
that his eyes see only the thing that he seeks,
and he is able to find nothing, to take in
nothing because he always thinks only about the thing he
is seeking, because he has one goal, because he
is obsessed with his goal. Seeking means: having a goal.
But finding means: being free, being open, having no goal.
-Hermann Hesse

Tornarem a sofrir,
tornarem a lluitar,
tornarem a guanyar.
-Lluís Companys

Winning isn't about finishing in first place.
It isn't about beating the others.
It is about overcoming yourself.
Overcoming your body, your limitations, and your fears.
Winning means surpassing yourself
and turning your dreams into reality.
-Kilian Jornet

Successful people are 100% convinced that
they are masters of their own destiny,
they're not creatures of circumstance,
they create circumstance, if the circumstances
around them suck, they change them.
-Jordan Belfort

To my family, because they have taught me *how* to think,
providing me the freedom to choose *what* to think.

Acknowledgements

Writing a thesis is very similar to sculpting a complex statue from a raw marble block. It is a tedious, slow and, above all, sometimes discouraging process. But if you keep fighting the adversities, keep focused, know your goals and pledge yourself to achieve them, I can tell you that, in the end, the feeling is extraordinarily beautiful.
I have always thought that *luck* is not something mystical that comes to you without any reason. Instead, I believe that luck is the reward that comes to you when something has been done correctly. In the end, if this premise is followed, luck might metamorphose into fame, money, recognition, love, or, simply, happiness. In my case, at this very moment of writing these words, luck has eventually transformed into *euphoria*.
I would like to express my deepest gratitude towards, Dr. Eusebi Calle, who has not only been the major advisor for my PhD, but has also been a mentor, guide, friend and paddle tennis mate.
I would like to thank all the members of the Broadband Communications and Distributed Systems research group, the Department of Computer Technology and Architecture, and the Institute of Informatics and Applications of the University of Girona.
I am equally grateful to Dr. Jose Alberto Hernández, Dr. Anna Manolova Fagertun and Dr. Caterina Scoglio, who invited me to work at their respective institutions. I also thank all my co-authors, for the lovely time spent together.
To conclude, I would like to thank Janus Friis and Niklas Zennström for bringing *Skype* into the world. Without this tool any of this would not have been possible.

This work has been partially supported by Spanish Ministry of Science and Innovation project TEC 2012-32336, and by the Generalitat de Catalunya research support program SGR-1202. This work has also been partially supported by the Secretariat for Universities and Research (SUR) and the Ministry of Economy and Knowledge through AGAUR FI-DGR 2012 and BE-DGR 2012 grants.

Barcelona, July 2014 M. M.

List of publications

- K. Bilal, S. U. Khan, M. Manzano, E. Calle, S. A. Madani, K. Hayat, D. Chen, L. Wang, and R. Ranjan. *Modeling and simulation of data center networks.* In S. U. Khan and A. Y. Zomaya, editors, Handbook on Data Centers. Springer-Verlag, New York, USA, 2014.

- K. Bilal, M. Manzano, E. Calle, C. Scoglio, and S. U. Khan. *Robustness Quantification of Hierarchical Complex Networks under Targeted Attacks.* 2013. Submitted to Physica A.

- K. Bilal, M. Manzano, S. U. Khan, E. Calle, Keqin Li , and A. Y. Zomaya. *On the characterization of the structural robustness of data center networks.* IEEE Transactions on Cloud Computing, 1(1):1–1, 2013.

- E. Calle, M. Manzano, and J. L. Marzo. *Multiple failures in telecommunication networks: robustness metrics and simulation tools.* In proceedings of the 2nd Workshop of Future Internet: Efficiency in high-speed networks (W-FIERRO 2012), 2012.

- E. Calle, J. Ripoll, J. Segovia, P. Vilà, and M. Manzano. *A multiple failure propagation model in GMPLS-based networks.* IEEE Network, 24(6):17– 22, 2010.

- M. Manzano. *Entorn de simulació de fallades per a xarxes òptiques de transport.* Final project of Computer Science Engineering Bachelor (3rd-year), University of Girona, 2009.

- M. Manzano. *Metrics to evaluate network robustness in telecommunications networks.* Final project of Computer Science Engineering Bachelor (5th-year), University of Girona & Strathclyde University, 2011.

- M. Manzano. *New Robustness Evaluation Mechanisms for Telecommunication Network Topologies.* Master's Thesis, University of Girona, 2012.

- M. Manzano, K. Bilal, E. Calle, and S.U. Khan. *On the connectivity of data center networks.* IEEE Communications Letters, 17(11):2172–2175, 2013.

- M. Manzano, E. Calle, and D. Harle. *Quantitative and qualitative network robustness analysis under different multiple failure scenarios.* In proceedings of the 3rd IEEE/IFIP International Workshop on Reliable Networks Design and Modelling (RNDM), 2011.

- M. Manzano, E. Calle, J. Ripoll, A. Manolova Fagertun, and V. Torres-Padrosa. *Epidemic Survivability: Characterizing Networks Under Epidemic-like Failure Propagation Scenarios.* In proceedings of the 9th International Conference on Design of Reliable Communication Networks (DRCN), 2013.

- M. Manzano, E. Calle, J. Ripoll, A. Manolova Fagertun, V. Torres-Padrosa, S. Pahwa, and C. Scoglio. *Epidemic and Cascading Survivability of Complex Networkss.* ArXiv e-prints 1405.0455, 2014. Submitted to International Journal of Communications, Network and System Sciences.

- M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, and D. Harle. *Endurance: A new robustness measure for complex networks under multiple failure scenarios.* Computer Networks, 57(17):3641–3653, 2013.

- M. Manzano, J.A. Hernandez, M. Urueña, and E. Calle. *An empirical study of cloud gaming.* In proceedings of the 11th Annual Workshop on Network and Systems Support for Games (NetGames), 2012.

- M. Manzano, J.A. Hernandez, M. Urueña, and E. Calle. *A first measurement study of online cloud gaming.* In proceedings of the 2nd Workshop of Future Internet: Efficiency in high-speed networks (W-FIERRO 2012), 2012.

- M. Manzano, J. L. Marzo, E. Calle, and A. Manolova. *Robustness analysis of real network topologies under multiple failure scenarios.* In proceedings of the 17th European Conference on Networks and Optical Communications (NOC), 2012.

- M. Manzano, A. Manolova Fagertun, S. Ruepp, E. Calle, C. Scoglio, A. Sydney, A. de la Oliva, and A. Muñoz. *Unveiling Potential Failure Propagation Scenarios in Core Transport Networks.* ArXiv e-prints 1402.2680, 2014. Submitted to IEEE Communications Magazine.

- A. Manolova Fagertun, S. Ruepp, and M. Manzano. *Resolving epidemic network failures through differentiated repair times.* IET Networks, 2014. Forthcoming.

- M. Manzano, J. Segovia, E. Calle, P. Vilà, and J. L. Marzo. *Modelling spreading of failures in GMPLS-based networks*. In proceedings of the 2010 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2010.

- M. Manzano, J. Segovia, E. Calle, and J. L. Marzo. *PHISON: Playground for High-level Simulations On Networks*. In proceedings of the 2012 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2012.

- M. Manzano, J. Segovia, E. Calle, and P. Vilà. *Failure propagation models for GMPLS-based networks*. In proceedings of the 2nd Workshop on Multilayer Networks: IP over Transport Networks, 2009.

- M. Manzano, F. Sahneh, C. Scoglio, E. Calle, and J. L. Marzo. *Robustness surfaces: a universal measure for complex networks*. In proceedings of the International School and Conference on Network Science (NetSci 2014), 2014.

- M. Manzano, F. Sahneh, C. Scoglio, E. Calle, and J. L. Marzo. *Robustness surfaces of complex networks*. ArXiv e-prints 1404.2403, 2014. Submitted to Scientific Reports.

- M. Manzano, V. Torres-Padrosa, and E. Calle. *Vulnerability of core networks under different epidemic attacks*. In proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modelling (RNDM), 2012.

- M. Manzano, M. Urueña, M. Suznjevic, E. Calle, J.A. Hernández, and M. Matijasevic. *Dissecting the protocol and network traffic of the onlive cloud gaming platform*. Multimedia Systems, 2014. Forthcoming.

- J. Ripoll, M. Manzano, and E. Calle. *Spread of epidemic-like failures in telecommunication networks*. Physica A, 410:457–469, 2014.

- I. Seoane, E. Calle, J.A. Hernández, J. Segovia, R. Romeral, P. Vilà, M. Urueña, and M. Manzano. *A CTMC-based characterisation of the propagation of errors in GMPLS Optical Rings*. In proceedings of the 9th Workshop in GMPLS networks (WGN9), 2010.

- I. Seoane, E. Calle, J.A. Hernández, J. Segovia, R. Romeral, P. Vilà, M. Urueña, and M. Manzano. *Failure propagation in GMPLS optical rings: CTMC model and performance analysis*. Optical Switching and Networking, 9(1):39–51, 2012.

- V. Torres-Padrosa, M. Manzano, E. Calle, and J. L. Marzo. *Community-based traffic preservation in telecommunication networks*. International Journal of Communication Systems, 2013. Forthcoming.

- V. Torres-Padrosa, M. Manzano, E. Calle, and J. L. Marzo. *Traffic-level community protection in telecommunication networks under large-scale failures*. In proceedings of the 2012 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2012.

Acronyms

IoT Internet of the Things

SID Susceptible-Infected-Disabled

GMPLS Generalized Multi-Protocol Label Switching

CTMC Continuous-Time Markov Chain

QNRM Quantitative Robustness Metric

QLRM Qualitative Robustness Metric

PHISON Playground for HIgh-level Simulations On Networks

ES Epidemic Survivability

EC Epidemic Criticality

HES High Epidemic Survivability

HESA High Epidemic Survivability Adaptive

ICT Information and Communication Technology

DCN Data Center Network

SDN Software-Defined Networking

SDNTN SDN-controlled Transport Network

BTN Backbone Transport Network

DTN Dynamic Transport Network

IP Internet Protocol

CS Cascading Survivability

MTTR Mean Time To Repair

QoS Quality of Service

SIS Susceptible-Infected-Susceptible

El Dr. Eusebi Calle, de la Universitat de Girona,

DECLARO:

Que el treball titulat "*New Robustness Evaluation Mechanisms for Complex Networks*", que presenta Marcos Manzano Castro per a l'obtenció del títol de doctor, ha estat realitzat sota la meva direcció i que compleix els requisits per poder optar a Menció Internacional.

I, perquè així consti i tingui els efectes oportuns, signo aquest document.

Signatura

Girona,

List of Figures

List of Tables

Compendium of publications

The following thesis is presented as a compendium of publications. The regulations for the requirements in the PhD technology program are the following:

- Three papers, of which one must be accepted in a first quarter journal or two accepted in second quarter journals.

The papers that meet the requirements are the following:

- M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, D. Harle. *Endurance: a new robustness measure for complex networks under multiple failure scenarios*. **Computer Networks**, Volume 57, Issue 17, Pages 3641-3653. (2013).
  DOI: http://dx.doi.org/10.1016/j.comnet.2013.08.011
  According to JCR 2012, Computer Networks has an Impact Factor of 1.231, is ranked 16/50, 47/132, 108/243 and 28/78 in the areas of "Computer science, hardware & architecture", "Computer science, information systems", "Engineering, electrical & electronic" and "Telecommunications", respectively, and belongs to Q2 in all of them.

- M. Manzano, K. Bilal, E. Calle, S. U. Khan. *On the Connectivity of Data Center Network*s. **IEEE Communications Letters**, Volume 17, Issue 11, Pages 2172-2175. (2013).
  DOI: http://dx.doi.org/10.1109/LCOMM.2013.091913.131176
  According to JCR 2012, IEEE Communications Letters has an Impact Factor of 1.160, is ranked 30/78 in the area of "Telecommunications", and belongs to Q2.

- Marc Manzano, Anna Manolova Fagertun, Sarah Ruepp, Eusebi Calle, Caterina Scoglio, Ali Sydney, Antonio de la Oliva, Alfonso Muñoz. *Unveiling Potential Failure Propagation Scenarios in Core Transport Networks*. Submitted to the IEEE Communications Magazine. (2014). http://arxiv.org/abs/1402.2680

Although the work carried out in this thesis has produced more than three articles (see Appendix), we would like to note that we have chosen the aforementioned papers for the compendium because:

- The PhD candidate is the corresponding author and, consequently, the first author.
- The three articles cover aspects on network science and networking, which are under a single topical umbrella.

Contents

Resum

La ciència de les xarxes (o *network science*) ha avançat significativament en l'última dècada, proporcionant coneixement sobre l'estructura subjacent i la dinàmica de les xarxes complexes (o *complex networks*). Infraestructures crítiques com xarxes de telecomunicacions, xarxes elèctriques o xarxes de transport, entre d'altres, són exemples de xarxes complexes omnipresents, ja que juguen un paper fonamental per garantir el bon funcionament de la vida moderna. Aquestes xarxes han de lidiar constantment amb fallades dels seus components. L'objecte del nostre estudi es centra principalment en les xarxes de telecomunicacions, encara que eventualment, en la fase final de la tesi, s'ha estès per tal de cobrir altres tipus de xarxes complexes.

A la literatura s'han proposat diverses estratègies per mitigar els efectes de les fallades simples (d'un sol component). No obstant això, hi ha un buit present en la literatura de les xarxes complexes pel que fa a escenaris de fallades múltiples, on els esquemes de protecció i restauració tradicionals no són adequats degut a la gran quantitat de recursos que serien necessaris. En aquests casos, el concepte de robustesa (o *robustness*) s'utilitza per tal de quantificar com de bona és una xarxa quan es produeix una fallada a gran escala.

L'objectiu d'aquesta tesi és, en primer lloc, investigar les amenaces actuals de les xarxes d'avui en dia que poden portar a escenaris de fallades múltiples i, en segon lloc, proposar nous indicadors capaços de quantificar la robustesa d'aquestes xarxes. Els treballs que s'han dut a terme durant aquesta tesi són el resultat d'una metodologia que s'ha basat en un increment de la complexitat gradual i la validació de resultats parcials a través de *peer-reviewing*. Com a conseqüència, d'una banda, s'han definit i estudiat diferents tipus d'escenaris de fallades múltiples, mentre que d'altra banda, hem proporcionant mètriques de robustesa aplicables als escenaris corresponents.

En aquesta línia, i en relació amb escenaris de fallades múltiples, s'identifiquen els errors dinàmics com un aspecte clau a tenir en compte. En particular, ens hem centrat en els errors de tipus epidèmic en xarxes de telecomunicacions. Per tant, una de les principals aportacions d'aquesta tesi està relacionada amb el modelatge de fallades múltiples. En aquest treball introduïm i refinem la precisió del model

epidèmic *Susceptible-Infected-Disabled* (SID), el qual s'aplica a la majoria dels nostres estudis de robustesa posteriors.
La part fonamental de les contribucions d'aquesta tesi és el conjunt de mètriques de robustesa que es proposen, les quals són capaces d'avaluar la robustesa de la xarxa sota escenaris de fallades múltiples. Alguns d'aquests indicadors es centren en nous escenaris de fallades múltiples (com epidèmies). D'altres, en canvi, són procediments genèrics adequats per avaluar la robustesa en qualsevol escenari de fallades múltiples i que, a més, es poden utilitzar per a aplicacions de monitorització en temps real.
Els resultats d'aquesta tesi mostren que algunes xarxes que són robustes quan es produeix un escenari de fallades múltiples, poden exhibir una alta vulnerabilitat sota altres escenaris. Aquest efecte depèn de la estructura subjacent de la xarxa, dels serveis que suporta aquesta, i del tipus d'escenari de fallada.

Resumen

La ciencia de la redes (o *network science*) ha avanzado significativamente en la última década, proporcionando conocimiento acerca de la estructura subyacente y la dinámica de las redes complejas (o *complex networks*). Infraestructuras críticas como redes de telecomunicaciones, redes eléctricas o redes de transporte, entre otras, son ejemplos de redes complejas omnipresentes, ya que juegan un papel fundamental para garantizar el buen funcionamiento de la vida moderna. Estas redes tienen que lidiar constantemente con fallos de sus componentes. El objeto de nuestro estudio se centra principalmente en las redes de telecomunicaciones, aunque eventualmente, en la fase final de la tesis, se ha extendido para cubrir otros tipos de redes complejas.

En la literatura se han propuesto varias estrategias para mitigar los efectos de los fallos simples (de un sólo componente). Sin embargo, existe un vacío presente en la literatura de las redes complejas con respecto a escenarios de fallos múltiples, donde los esquemas de protección y restauración tradicionales no son adecuados debido a la gran cantidad de recursos que serían necesarios. En estos casos, el concepto de robustez (o *robustness*) se utiliza con el fin de cuantificar cómo de buena es una red cuando se produce un fallo a gran escala.

El objetivo de esta tesis es, en primer lugar, investigar las amenazas actuales de las redes de hoy en día que pueden llevar a escenarios de fallos múltiples y, en segundo lugar, proponer nuevos indicadores capaces de cuantificar la robustez de estas redes. Los trabajos que se han llevado a cabo durante esta tesis son el resultado de una metodología que se ha basado en un incremento de la complejidad gradual y la validación de resultados parciales a través de *peer-reviewing*. Como consecuencia, por un lado, se han definido y estudiado diferentes tipos de escenarios de fallos múltiples, mientras que por otro lado, hemos proporcionando métricas de robustez aplicables a los escenarios correspondientes.

En esta línea, y en relación con escenarios de fallos múltiples, se identifican los fallos dinámicos como un aspecto clave a tener en cuenta. En particular, nos hemos centrado en los fallos de tipo epidémico en redes de telecomunicaciones. Por lo tanto, una de las principales aportaciones de esta tesis está relacionada con el modelado

de fallos múltiples. En este trabajo introducimos y refinamos la precisión de el modelo epidémico *Susceptible-Infected-Disabled* (SID), el cual se aplica a la mayoría de nuestros estudios de robustez posteriores.
La parte fundamental de las contribuciones de esta tesis es el conjunto de métricas de robustez que se proponen, las cuales son capaces de evaluar la robustez de la red bajo escenarios de fallos múltiples. Algunos de estos indicadores se centran en nuevos escenarios de fallos múltiples (como epidemias). El resto de métricas propuestas son procedimientos genéricos adecuados para evaluar la robustez en cualquier escenario de fallos múltiples y que, además, se pueden utilizar para aplicaciones de monitoreo en tiempo real.
Los resultados de esta tesis muestran que algunas redes que son robustas cuando se produce un escenario de fallos múltiples, pueden exhibir una alta vulnerabilidad bajo otros escenarios. Este efecto depende de la estructura subyacente de la red, de los servicios que soporta ésta, y del tipo de escenario de fallo.

Abstract

Network science has significantly advanced in the last decade, providing insights into the underlying structure and dynamics of complex networks. Critical infrastructures such as telecommunication networks, power grids or transportation networks, among others, are complex networks which are omnipresent and play a pivotal role in ensuring the smooth functioning of modern day living. These networks have to constantly deal with failures of their components. Our focus is primarily on telecommunication networks, although eventually it has been extended to cover other types of complex networks.

Several strategies to mitigate the effects of single failures have been proposed in the literature. However, there is a present gap in the complex networks domain, with respect to multiple failure scenarios, where traditional protection and restoration schemes are not suitable because of the quantity of resources that would be required. In these cases, different strategies are needed to mitigate the effects of multiple failures. The concept of *robustness* is used in order to quantify just how good a network is under a large-scale failure scenario.

The aim of this thesis is to, firstly, investigate the current challenges that might lead to multiple failure scenarios of present day networks and, secondly, to propose novel metrics able to quantify the network robustness. In addition, the research works leading to this thesis are the result of a methodology that has been based on the incremental complexity and the validation of partial results via peer-reviewing. As a consequence, on the one hand we defined and studied different types of multiple failure scenarios while, on the other hand, we provided robustness metrics applicable to the corresponding scenarios.

Along these lines, and concerning multiple failure scenarios, we identify the dynamic failures as a key aspect to take into account. In particular, we have focused on epidemic-like failures in telecommunication networks. Therefore, one of the major contributions of this thesis is related to the modelling of multiple failures. We introduce and refine the accuracy of the Susceptible-Infected-Disabled (SID) epidemic model, which is then applied to the majority of our subsequent robustness

studies.
The fundamental part of our contributions is the set of robustness metrics that are proposed and which are able to assess network robustness under multiple failure scenarios. Some of these metrics are focused on new multiple failure scenarios (such as epidemics), while the rest of the proposed metrics are generic procedures suitable for assessing network robustness under any given multiple failure scenario and, what is more, can be used for real-time monitoring applications.
The results of this thesis show that some networks that are robust under a given multiple failure scenario, can reveal a high vulnerability under other scenarios. This effect depends on the underlying network structure, the services running over such networks and the type of failure scenario.

General Introduction Part I

1 Introduction

The purpose of this chapter is to (a) outline the motivation for the work conducted in this thesis; (b) present an overview of the topics in which this thesis is categorised; and (c) describe the background and previous publications of the research work.

1.1 Motivation

Our civilization is going through an extraordinary and unstoppable evolution. Such development is strongly related with the constant flourishing of new technologies and the tremendous progresses that have been done in science in the past decades.

Networks are partially responsible for the blossoming of the modern society: from the first transcontinental railway networks that were built in the 19th century, including the appearance of power grids and water distribution networks, to more recent systems such as telephone networks, or the Internet. In addition, we will soon witness the new era of the Internet of Things (IoT), where every single element or human being will be connected to one another. Unquestionably, the tendency of our civilization is to depend more and more on networks.

The Committee on Network Science for Future Army Applications defines a *network* "*by its structure (e.g., nodes and links), and its behaviour (what the network does as a result of the interactions among the nodes and links). A network is always a representation or model of observable reality, not the reality itself*" [Lew09]. For instance, societies are networks of people linked by friendships, or the brain is a network of nerve cells connected by axons. Many large-scale real-world networks present an underlying complex structure. Such networks have been referred to as *complex systems* or *complex networks*. A comprehensive and detailed explanation of what a *complex network* is can be found in [Ste10]. According to van Steen, a complex network is "*a*

large collection of interconnected nodes". Therefore, as it turns out, complex networks are everywhere (e.g., computer networks or online social networks).

The study of complex networks has attracted significant attention in the past decade. Critical infrastructures such as telecommunication networks, power grids or transportation networks, among others, are complex networks which are omnipresent and play a pivotal role in ensuring the smooth functioning of modern day living. Such networks have to constantly deal with failures of their components. As a consequence, any disruption of the service provided might have a considerable impact upon sizable proportions of the world's inhabitants. Thus, there are two aspects involved in the study of complex networks that are of paramount importance:

1. The study of the structure of a collection of nodes and links.

2. The study of the dynamic behavior (or dynamic phenomena) of the aggregation of nodes and links.

This thesis has addressed both aspects. In addition, it has been mostly focused on telecommunication networks. However, at its last stage, the range of considered networks has been significantly enlarged by several works.

1.2 Covered topics

Fig. 1.1 shows a diagram where the main covered topics of this thesis are presented. This thesis belongs to the *network science* research field. Network science, or the *science of networks*, is defined as "*the study of the theoretical foundations of network structure/dynamic behavior and the application of networks to many subfields, such as social network analysis, collaboration networks (bibliographic citations), synthetic emergent systems (power grids, the Internet, etc.), physical science systems (phase transition, percolation theory, etc.), and life systems (epidemics, genetics, etc.).*", according to Lewis [Lew09].

The diagram depicts a unidirectional relationship of five topics: four being the input of a fifth. This layout can be explained backwards. The main topic of this thesis is the *robustness of complex networks*. Robustness is defined as the ability of a network to maintain its total throughput under node or link removal [SSYS10].

In order to characterise the network robustness, one should take into account several aspects:

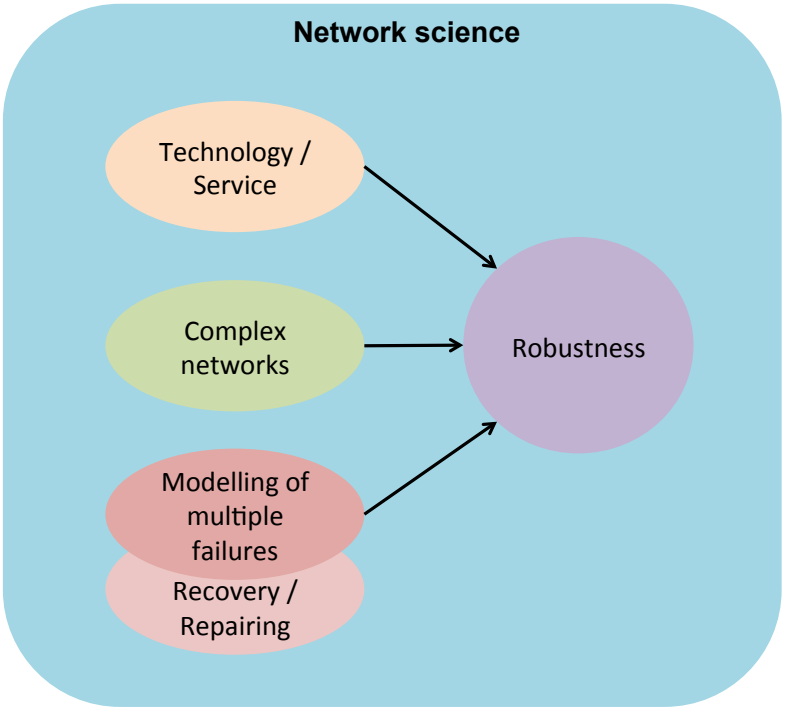


Figure 1.1: Topics covered in this thesis

- What type of network is to be studied.
- The target of the assessment: whether it is going to be the underlying physical structure or the service provided by the network.
- What kind of failures occur. In this thesis we focus on multiple failure scenarios.
- What recovery mechanisms are to be applied after a failure.

Each of these four aspects constitute a whole block of study. Therefore, we have studied the robustness of complex networks considering the following four topics:

- Technology / Service: Mainly focused on telecommunication networks, this block defines which telecommunication network technologies have been considered, as well as which specific type of networks. In addition, it specifies whether the objective of the study has been to analyze the connections or the physical connectivity instead.
- Complex networks: Defines what type of networks have been considered.
- Modelling of multiple failures: Describes the taxonomy of failures that has been used in this thesis.

- Recovery / Repairing: Partially intersecting with the previous topic, this block would not be relevant without its failures counterpart. It presents a few strategies that have been considered under a specific scenario of multiple failures. This is the topic that has been addressed in a least extent, due to the fact that recovery or repairing strategies cannot be applied under the majority of multiple failure scenarios.

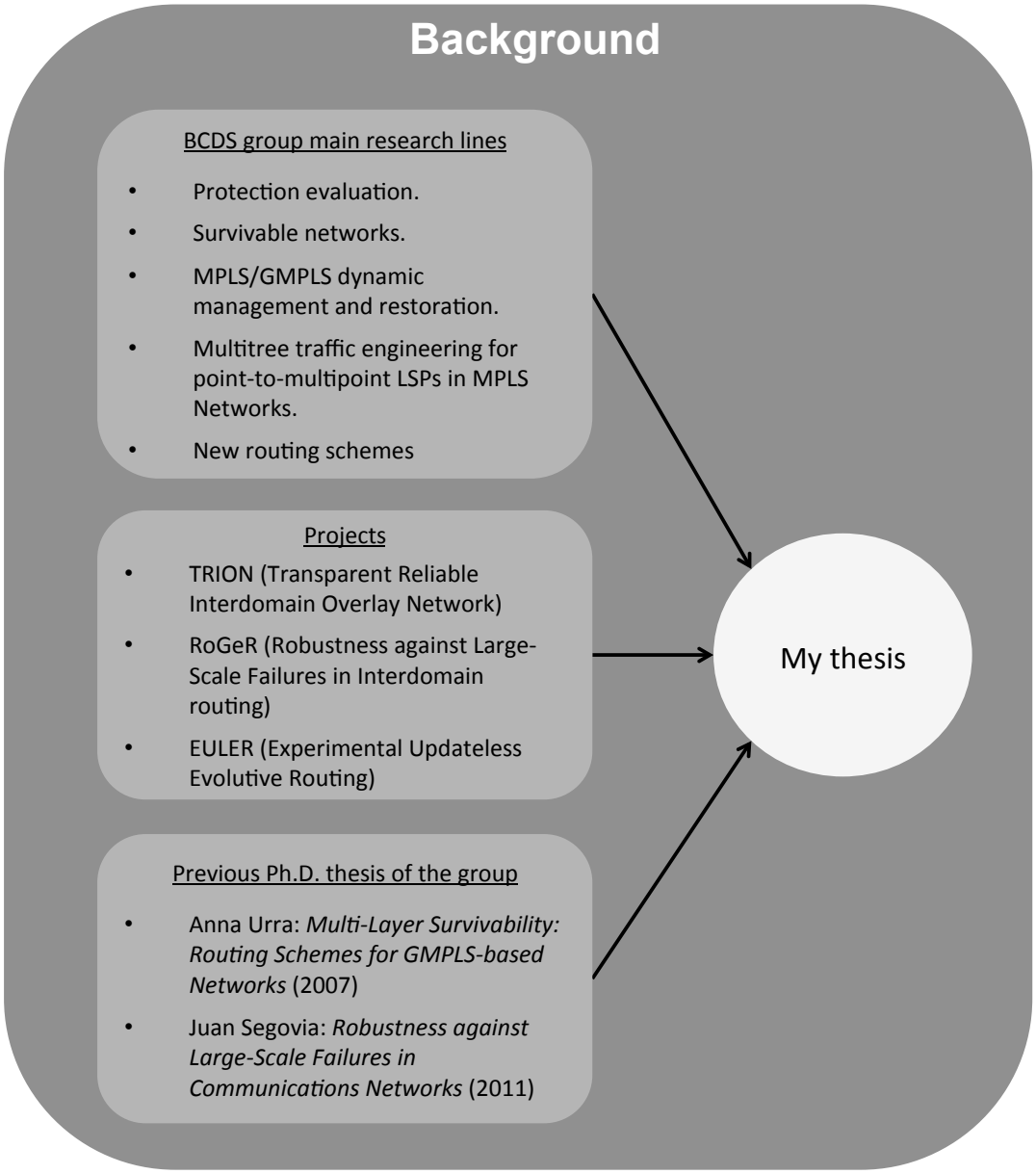


Figure 1.2: Background of the doctoral thesis: *where does it come from?*

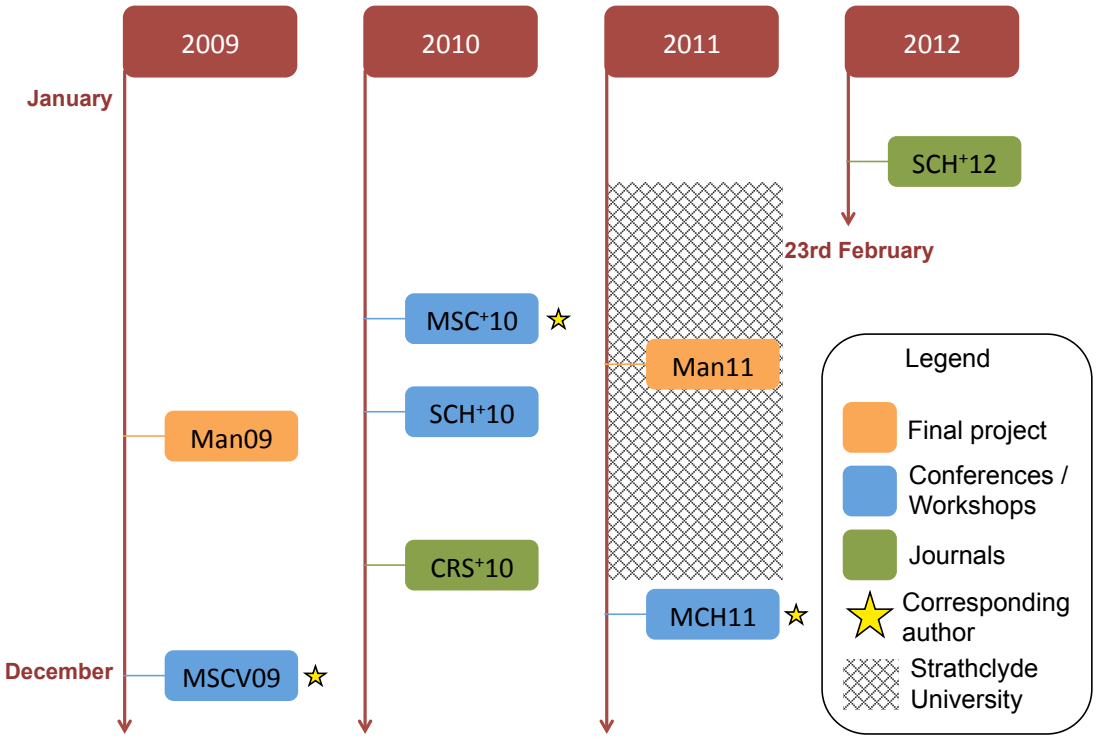


Figure 1.3: Timeline chart before starting the doctoral thesis.

1.3 Background

"*Where does this thesis come from?*" Fig. 1.2 presents the three reasons that defined the frame in which the research conducted in this work was initiated. As observed, this work has been done within the Broadband Communications and Distributed Systems (BCDS) research group of the University of Girona. The main research lines of the BCDS group constituted a firm foundation for the work that has been done in this thesis. In addition, the projects in which the group was involved provided additional value to the research that was done. Finally, the foremost reasons that triggered this work were the two theses shown at the lowest part of Fig. 1.2. The theses of Dr. Anna Urra and Dr. Juan Segovia have been the source this work has been inspired from.

To complement the information regarding the background of this thesis, Fig. 1.3 shows a timeline chart of the different projects and articles that were done before starting the doctoral thesis. The diagram shows vertically the years that have comprised this phase. As depicted, the final project of the technical Computer Science Engineering Bachelor (a 3-year degree) was the first work that was done [Man09]. In such project, we presented the *Susceptible-Infected-Disabled* (SID) epidemic model, which was used to evaluate the robustness of GMPLS-based (Generalised Multi-Protocol Label

Switching) networks. Further results originating from the project were presented at the *2nd Workshop on Multilayer Networks: IP over Transport Networks* [MSCV09] and the *2010 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)* [MSC+10], the latter being the first international conference to which one of our works was presented. Next, we defined a Continuous-Time Markov Chain (CTMC) model to characterise the propagation of failures in optical GMPLS-based rings, which was presented at the *9th Workshop in GMPLS networks (WGN9)* [SCH+10]. This was the first work which was done in collaboration with another institution. Our first journal paper was published in the *IEEE Network* magazine, and defined more rigorously the SID model [CRS+10]. Later on, in the final project of the Computer Science Engineering Bachelor two new robustness metrics were presented: the *Quantitative Robustness Metric* (QNRM) and the *Qualitative Robustness Metrics* (QLRM) [Man11]. Further results were then presented at the *3rd International Workshop on Reliable Networks Design and Modeling (RNDM)* [MCH11]. Finally, we extended the study carried out in [SCH+10] by providing a set of guidelines for selecting appropriate repairing rates to attain specific availability requirements. The results were published in the *Optical Switching and Networking* journal [SCH+12].

2 Objectives

The main objective of this thesis is to investigate, propose and validate new robustness evaluation mechanisms for complex networks.

Our focus has been mainly on telecommunication networks, although different types of complex networks have been considered at the last stage of the thesis.

The technical objectives of the thesis are to:

- Model multiple failure scenarios. A taxonomy should be proposed in order to differentiate the distinct failure scenarios (e.g., static or dynamic).
- Design and implement a network simulator able to work with large networks (thousands of nodes). The simulator should allow the user to cause multiple failures. As a consequence, how the service provided by the network is affected under such failure scenarios must be studied.
- Propose, develop, and validate new measures allowing network operators and engineers to assess the network robustness on real time.
- Present a categorization of the different robustness degrees that distinct complex networks have.

3 Methodology, tools and contributors

The aim of this chapter is to (a) reveal the methodology that has been followed in this thesis; (b) present the tools that have been used; and (c) enumerate the different collaborators without whom this thesis would not have been possible.

3.1 Methodology

The methodology that has been adopted in this thesis is the incremental complexity and the validation of partial results via peer-reviewing. As a consequence, this period has been highly productive with respect to the number of manuscripts that have been published in both international journals or conferences. Fig. 3.1 presents a timeline chart of the period comprising the thesis.

Following our methodology, we have presented preliminary results to international conferences or workshops because the peer-review process requires significantly less time than for international journals. This has allowed us to receive feedback in order to improve and mature our contributions, which then have been sent to journals. As a consequence, two trends are clearly distinguishable: the first year has been mainly focused to publish our results in well-known international conferences or workshops, while the rest of the period has been focused on international journals.

In addition, it can also be noted that three stays have been done at University Carlos III of Madrid (Spain), at the Technical University of Denmark (Denmark) and at Kansas State University (USA). These stays have triggered the collaboration with several researchers (see section 3.3).

As mentioned in chapter 2, the network robustness and the modelling of multiple failure scenarios have been the central part of this thesis. The publications that are

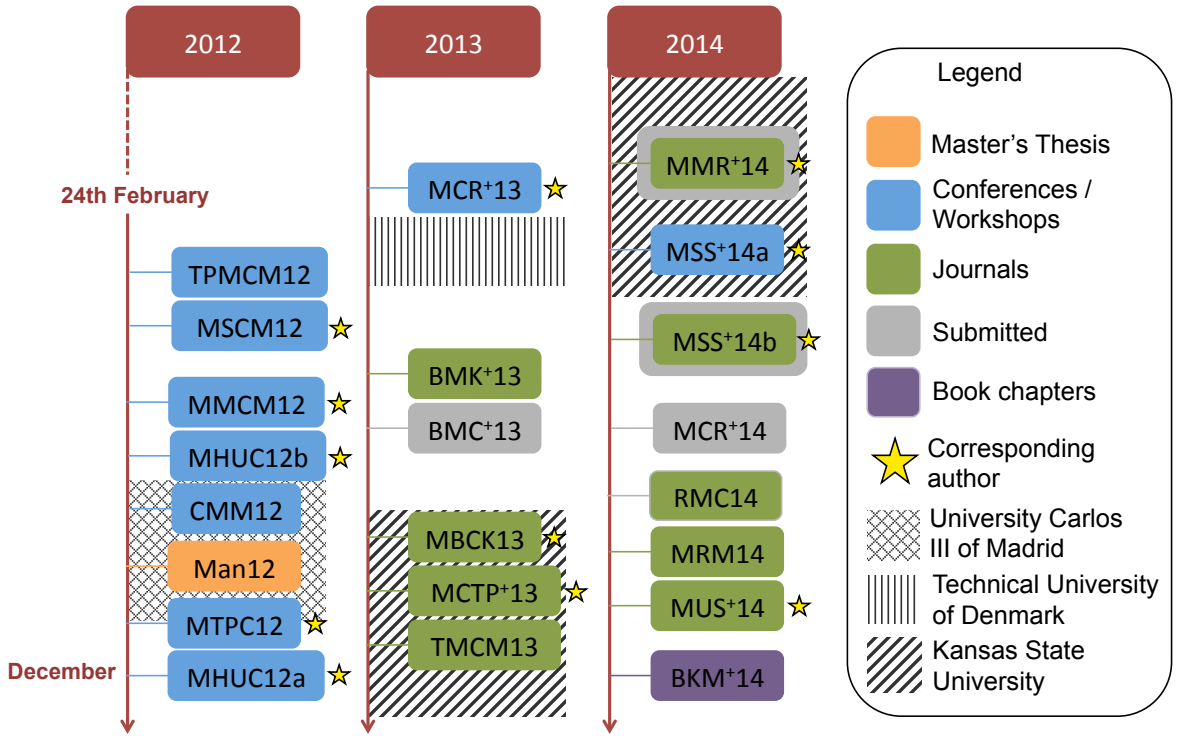


Figure 3.1: Timeline chart of the doctoral thesis

described from now on provide contributions related to these two lines.

The first paper to be published within the period of this thesis was [TPMCM12]. It was presented at the *2012 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*. In such paper we proposed a new method to detect communities (a set of nodes with a common characteristic: e.g., a network region with high edge density), which is based on the traffic that is exchanged between the nodes of a given network. Results showed that it is possible to preserve the connections within a community, or between communities, depending on which nodes are protected. Simultaneously, at the same conference, we presented the first version of our discrete-event network simulator, PHISON (Playground for HIgh-level Simulations On Networks) [MSCM12] (see section 3.2). The publication of our own simulation tool was indispensable in order to continue our research, and fulfill one of the objectives of this thesis. Then, a robustness analysis of several real telecommunication networks was presented to the *17th European Conference on Networks and Optical Communications (NOC)* [MMCM12]. Results showed that, according to the *QNRM* and *QLRM* robustness metrics, some real telecommunication networks are robust in response to a specific type of failure.

In parallel, during a research stay at the University Carlos III of Madrid, we studied a

well-known cloud gaming platform (OnLive) and conducted a traffic measurement analysis. The purpose of the paper was to compare the traffic generated by traditional gaming platforms (such as Xbox or Play Station) with the new cloud gaming platforms. This study complements the whole topic of this thesis with a real service analysis of the contemporary telecommunication networks. The results were presented at the *2nd Workshop of Future Internet: Efficiency in high-speed networks (W-FIERRO 2012)* [MHUC12b]. At the same time, an overview of the research that was being conducted within the BCDS research group at the University of Girona was presented [CMM12].

The work that was done for the Master's thesis [Man12] lighted the spark and initiated several works the came *a posteriori*: we rigorously investigated the robustness of complex networks under epidemic-like failure scenarios, and proposed a generic method to characterise the network robustness, regardless of the failure scenario.

At the *4th IEEE/IFIP International Workshop on Reliable Networks Design and Modelling (RNDM)* we presented an article where we conducted a robustness analysis of real core telecommunication networks under different epidemic-like attacks [MTPC12]. This was the first targeted-based study of complex networks under failure propagation scenarios. In this case, we were selecting according to several criteria the nodes that were initially infected, and that started to propagate the failure (or infection). Results revealed that core telecommunication networks react differently depending on the type of epidemic failure. Additionally, we provided a study of the repairing times needed to eradicate the different types of epidemics. We showed that depending on the physical structure of some real networks, a higher cost might be required in order to maintain an acceptable level of service.

A more detailed traffic analysis of cloud gaming platforms than the one done in [MHUC12b] was presented at the *11th Annual Workshop on Network and Systems Support for Games (NetGames)* [MHUC12a]. In this paper we provided an overview of the traffic generated by two cloud gaming platforms: OnLive and Gaikai.

The feedback received while presenting [MTPC12] allowed us to define and propose a new network measure called *Epidemic Survivability* (ES), which is able to characterise the vulnerability of each node of the network under an epidemic-like failure scenario. Furthermore, we used *ES* to propose:

- *Epidemic Criticality* (EC): a robustness measure for dynamic multiple scenarios.
- Two new network immunization strategies, *High Epidemic Survivability* (HES) and *High Epidemic Survivability Adaptive* (HESA).

These contributions were presented at the *9th International Conference on Design of Reliable Communication Networks (DRCN)*, where the manuscript was nominated to the *best paper award* [MCR+13]. Results showed that *EC* is able to differentiate the criticality of two different networks for a specific epidemic scenario. Moreover, it was shown that HESA outperformed traditional immunization techniques.

With the advent of cloud computing and the fact that it is integral to the Information and Communication Technology (ICT) sector, we decided to focus part of our study to Data Center Networks (DCNs). DCNs constitute the communicational backbone of the cloud, and hold a pivotal role to ascertain the data center performance and integrity. Given that a minor degradation of the service would result in enormous losses, DCNs need to be robust to failures. In our manuscript published in the *IEEE Transactions on Cloud Computing* journal [BMK+13], we proposed a mathematical definition of DCNs, and we evaluated the structural robustness of such networks under random failures and targeted attacks. Thereafter, we aimed to emphasise the relationship between the network hierarchy and robustness, and we submitted the findings to the *Physica A* journal [BMC+13].

To complement the contributions presented in [BMK+13], the connectivity of DCNs was evaluated and characterised via the μ*-A2TR* metric (Average Two-Terminal Reliability). The results were published in the *IEEE Communications Letters* journal [MBCK13].

At the same time we started to work on the proposal of a generic robustness measure. The observations and valuable comments that were received by presenting [MCH11, MMCM12, MTPC12, MCR+13] inspired us to eventually present *endurance*, which quantifies the level of robustness supported by a specific network topology under different types of multiple failure scenarios, giving higher importance to perturbations affecting low percentages of elements of a network. The outcome of this study was published in the *Computer Networks* journal [MCTP+13]. Besides presenting *endurance*, in this paper we proposed a taxonomy to classify the different types of multiple failure scenarios. Results showed that the *endurance* is able to describe the robustness of a network under different multiple failure scenarios.

Simultaneously, we extended the article presented in [TPMCM12] according to the feedback that was given by the reviewers, and presented a more detailed and thorough study, which was accepted for publication in the *International Journal of Communication Systems* [TMCM13].

At that point, there was a comment that was done at every single conference/workshop venue where we presented our robustness-related works: "(a) Are epidemic-like

failures possible in core/backbone telecommunication networks? (b) There is no real data supporting your hypotheses. (c) How can you study a failure scenario that is not possible?". With the objective of being able to answer these questions, we decided to conduct the following study. Given that Software Defined Networking (SDN) was becoming more prevalent in our society, it would not be surprising to experience the proliferation of SDN-controlled Transport Networks (SDNTNs). While doing a research stay at the Technical University of Denmark, we coordinated a multi-institutional study investigating the main motivations that could lead to epidemic-like failures in Backbone Transport Networks (BTNs) and SDNTNs. To do so, we enlisted the expertise of several research groups with significant background in epidemics, network resiliency, and security. In addition, we considered the experiences of three network providers. The article was submitted to the *IEEE Communications Magazine* [MMR+14]. Results showed that Dynamic Transport Networks (DTNs) (e.g., GMPLS-based transport networks) are prone to epidemic-like failures. In addition, we proposed several situations in which a failure can propagate in SDNTNs.

Later on, while doing a research stay at Kansas State University, we solved two open issues in the network robustness literature: (a) how to dimension several robustness metrics to allow their summation and (b) how to weight each of the metrics. Our contributions were the R^*-value and the concept of *robustness surfaces* (Ω). The former extracts the most informative robustness metric for a failure scenario (i.e., type of failure and attack strategy), while the latter allows network robustness variations of different networks to be visually assessed, regardless of the failure scenario. Partial results were presented at the *International School and Conference on Network Science (NetSci 2014)* [MSS+14a], and with the received feedback from several researchers that got interested in our work, we conducted the entire study and it was submitted to the *Scientific Reports* [MSS+14b]. Results showed that a network presents different robustness surfaces (i.e., dissimilar shapes) depending on the failure scenario and the set of metrics. In addition, the robustness surface allows the robustness of different networks to be compared. In fact, robustness surfaces are designed as a visual monitoring tool. First, our approach is applicable to real-time monitoring of a network through a single value, when it is otherwise implemented according to multiplicity of correlated metrics with possible inherent redundancy. Second, Ω can be a pivotal part of a network robustness refinement process:

- Step 1: If the robustness surface presents abrupt slopes, then there are network elements (nodes or links) which are weaker than the rest, for a given failure scenario. These elements could be identified by means of traditional robustness metrics such as the betweenness centrality.

- Step 2: Enhance or protect the weak elements, for instance, by adding new links or applying immunization techniques.
- Step 3: Re-evaluate the robustness of a network and, instead of comparing a large number of robustness metrics, detect through visual inspection if the network robustness has been improved.

Besides, we extended the study presented in [MCR+13], as suggested in the peer-review process, by considering a wider range of complex networks, as well as proposing a new measure called *cascading survivability*. The scope of the study was to consider the two major dynamic multiple failure scenarios: epidemic and cascading-like failure propagation scenarios. Results were submitted to the *International Journal of Communications, Network and System Sciences* [MCR+14], and showed that distinct types of complex networks might react differently under dynamic multiple failure scenarios.

Furthermore, we carried out a more thorough study of the SID epidemic model, which was previously presented in [MSCV09, MSC+10, CRS+10]. The main reason that triggered this new work was that we observed a difference between the predicted results of the analytical model and the simulations. As a consequence, we compared the accuracy of the numerical results obtained from the SID epidemic model with the results that were obtained from simulations, which resulted to be different depending on the type of network. To improve the level of accuracy, we proposed a slight modification of the equations describing the model. Finally, we obtained much more refined predictions. These results were published in the *Physica A* journal [RMC14].

In addition, we studied the strategic placement of recovery resources in a GMPLS-based network, when epidemic-like failures occur. Results showed that the strategic placement of recovery resources has better performance than randomly assigning lower repair times. Moreover, it was shown that an event-driven simulation model can be highly beneficial for network providers, since it could be used during the network planning process for facilitating cost-effective network survivability design. These contributions were presented in the *IET Networks* journal [MRM14].

During the peer-review process of [MHUC12b, MHUC12a] we where asked to compare in depth different cloud gaming platforms. However, comparing two different cloud gaming platforms first requires the understanding of the employed protocols, and since most protocols used by the cloud gaming providers are proprietary, the only way to understand them is by reverse engineering. Consequently, we carried out a rigorous reverse-engineering study of the protocol of the OnLive cloud gaming platform. Additionally, we presented a network traffic model in order to allow network operators

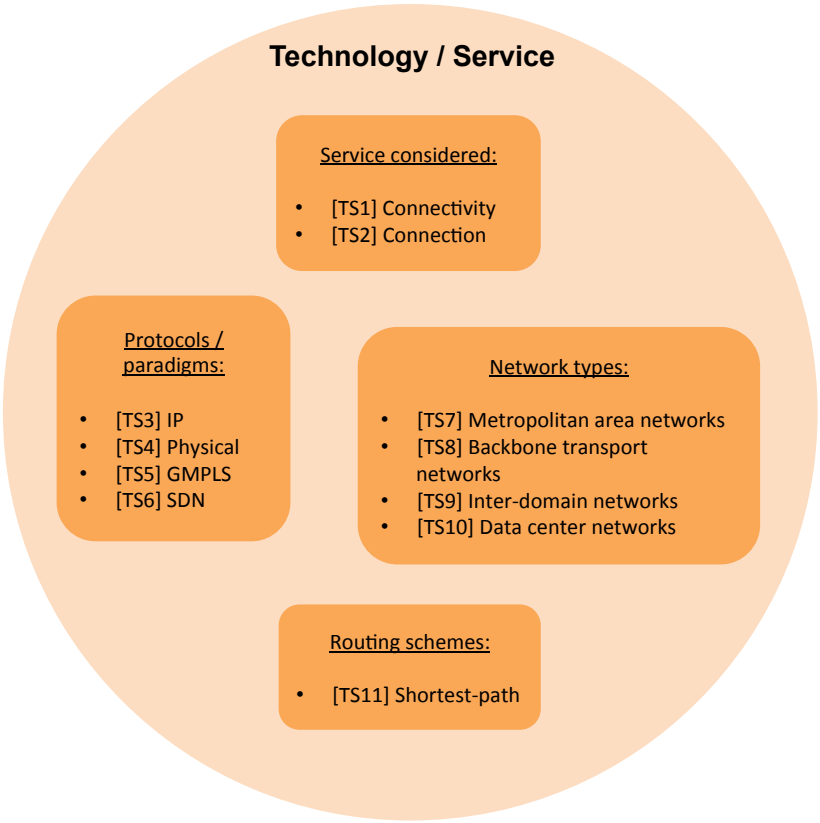


Figure 3.2: Technology / Service.

to design and give the proper dimension to future networks. These contributions were published in the *Multimedia Systems* journal [MUS+14].

To conclude, we cooperated with several researchers in order to write a book chapter about DCNs, which was published in the *Handbook on Data Centers*, of *Springer-Verlag* [BKM+14].

3.1.1 Relationship between the articles and the covered topics

In chapter 1, section 1.2, an overview of the main topics that this thesis has covered has been presented. Here, we detail each of the blocks shown in Fig. 1.1, and we associate each of the subtopics of each block to the articles that have been listed in the previous section. We believe that the dissection provided below gives a thorough overview of this thesis.

The first block is shown in Fig. 3.2, which relates to *Technology* and *Service*. As observed, it is divided into four areas: the service considered, protocols and paradigms, networks types and routing schemes. Each of the subtopics within those areas have

Table 3.1: Articles that have covered topics of *Technology / Service*.

Subtopics	Articles
[TS1]	[Man11, MCH11, TPMCM12, MSCM12, MMCM12, CMM12, Man12, MTPC12, MCR$^+$13, BMC$^+$13, BMK$^+$13, MBCK13, MCTP$^+$13, MSS$^+$14a, MSS$^+$14b, MCR$^+$14]
[TS2]	[Man09, MSCV09, MSC$^+$10, SCH$^+$10, CRS$^+$10, Man11, MCH11, SCH$^+$12, TPMCM12, MSCM12, MMCM12, CMM12, Man12, MRM14, MCTP$^+$13, TMCM13]
[TS3]	[Man11, MCH11, MMCM12, MHUC12b, MTPC12, MHUC12a, MCR$^+$13, BMC$^+$13, RMC14, BMK$^+$13, MBCK13, TMCM13, MMR$^+$14, MUS$^+$14, BKM$^+$14]
[TS4]	[Man11, MCH11, TPMCM12, MMCM12, Man12, MTPC12, BMC$^+$13, RMC14, BMK$^+$13, MBCK13, TMCM13, MCR$^+$14]
[TS5]	[Man09, MSCV09, MSC$^+$10, SCH$^+$10, CRS$^+$10, SCH$^+$12, Man12, MRM14, MMR$^+$14]
[TS6]	[MMR$^+$14]
[TS7]	[SCH$^+$10, SCH$^+$12, MHUC12b, MHUC12a, MUS$^+$14]
[TS8]	[Man11, MCH11, TPMCM12, MMCM12, MHUC12b, Man12, MTPC12, MHUC12a, MCR$^+$13, RMC14, MRM14, TMCM13, MMR$^+$14, MUS$^+$14, MCR$^+$14]
[TS9]	[Man09, MSCV09, MSC$^+$10, Man11, MCH11, MHUC12b, MHUC12a, BMC$^+$13, MUS$^+$14]
[TS10]	[MHUC12b, MHUC12a, BMC$^+$13, BMK$^+$13, MBCK13, MUS$^+$14, BKM$^+$14]
[TS11]	[Man09, MSCV09, MSC$^+$10, SCH$^+$10, CRS$^+$10, Man11, MCH11, TPMCM12, MMCM12, Man12, MCTP$^+$13, TMCM13]

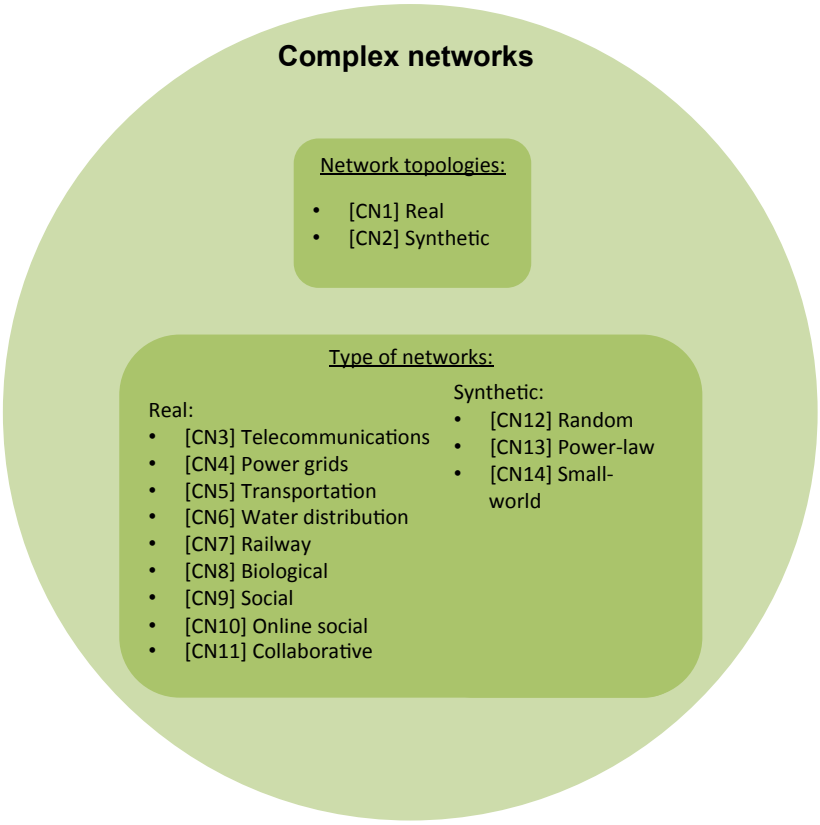


Figure 3.3: Complex networks.

been labeled. Table 3.1 presents a classification of which of our articles have addressed a specific subtopic.

The second block, about *Complex Networks*, is shown in Fig. 3.3. It aims to classify the different network topologies that have been used in this thesis. As observed, they can be either real or synthetic.

Most of the real telecommunication networks that we have worked with are from the Internet topology zoo, which can be found at http://www.topology-zoo.org/. The rest of real networks have been obtained by contacting the authors of several works that were presenting such network topologies, from the DIMES project (http://www.netdimes.org) or the SNAP project (http://snap.stanford.edu).

Regarding the synthetic networks, we have mainly considered three types: random, power-law and small-world networks.

The Erdős-Rényi (ER) model [Bol01] is related with *random networks*. The term "random" refers here to the fact that, during the generation of a graph instance, the arrangement of links is disordered. Random networks are a primitive and crude

Table 3.2: Articles that have covered topics of *Complex networks*.

Subtopics	Articles
[CN1]	[SCH$^+$10, Man11, MCH11, TPMCM12, MSCM12, MMCM12, MHUC12b, CMM12, Man12, MTPC12, MHUC12a, MCR$^+$13, BMC$^+$13, RMC14, BMK$^+$13, MRM14, MBCK13, TMCM13, MMR$^+$14, MSS$^+$14a, MSS$^+$14b, MUS$^+$14, MCR$^+$14, BKM$^+$14]
[CN2]	[Man09, MSCV09, MSC$^+$10, CRS$^+$10, Man11, MCH11, TPMCM12, MSCM12, CMM12, Man12, MCR$^+$13, BMC$^+$13, RMC14, MCTP$^+$13, TMCM13]
[CN3]	[SCH$^+$10, Man11, MCH11, SCH$^+$12, TPMCM12, MSCM12, MMCM12, MHUC12b, CMM12, Man12, MTPC12, MHUC12a, MCR$^+$13, BMC$^+$13, RMC14, BMK$^+$13, MRM14, MBCK13, TMCM13, MMR$^+$14, MUS$^+$14, MCR$^+$14, BKM$^+$14]
[CN4]	[BMC$^+$13, MSS$^+$14b, MCR$^+$14]
[CN5]	[BMC$^+$13, MCR$^+$14]
[CN6]	[MCR$^+$14]
[CN7]	[MSS$^+$14a, MSS$^+$14b]
[CN8]	[MCR$^+$14]
[CN9]	[MCR$^+$14]
[CN10]	[MCR$^+$14]
[CN11]	[MCR$^+$14]
[CN12]	[Man11, MCH11, TPMCM12, MSCM12, CMM12, Man12, MCR$^+$13, RMC14, MCTP$^+$13, TMCM13]
[CN13]	[Man09, MSCV09, MSC$^+$10, Man11, MCH11, TPMCM12, Man12, MCR$^+$13, BMC$^+$13, RMC14, MCTP$^+$13, TMCM13]
[CN14]	[Man11, MCH11, Man12, MCR$^+$13, MCTP$^+$13]

Table 3.3: Articles that have covered topics of *Modelling of multiple failures* and *Modelling of recovering policies*.

Subtopics	Articles
[MMF1]	[Man09, MSCV09, MSC$^+$10, SCH$^+$10, CRS$^+$10, Man11, MCH11, SCH$^+$12, TPMCM12, MSCM12, MMCM12, CMM12, Man12, MTPC12, MCR$^+$13, BMC$^+$13, RMC14, BMK$^+$13, MRM14, MBCK13, MCTP$^+$13, TMCM13, MMR$^+$14, MSS$^+$14b, MCR$^+$14]
[MMF2]	[MSS$^+$14a, MSS$^+$14b]
[MMF3]	[Man09, MSCV09, MSC$^+$10, SCH$^+$10, CRS$^+$10, Man11, MCH11, SCH$^+$12, TPMCM12, MMCM12, CMM12, Man12, MTPC12, MCR$^+$13, BMC$^+$13, RMC14, BMK$^+$13, MRM14, MBCK13, MCTP$^+$13, TMCM13, MMR$^+$14, MSS$^+$14a, MSS$^+$14b, MCR$^+$14]
[MMF4]	[TPMCM12, MSCM12, CMM12, Man12, MTPC12, MCR$^+$13, BMC$^+$13, BMK$^+$13, MBCK13, MCTP$^+$13, MMR$^+$14, MSS$^+$14a, MSS$^+$14b]
[MMF5]	[Man11, MCH11, TPMCM12, MSCM12, MMCM12, CMM12, Man12, MCR$^+$13, BMC$^+$13, BMK$^+$13, MBCK13, MCTP$^+$13, TMCM13, MMR$^+$14, MSS$^+$14a, MSS$^+$14b]
[MMF6]	[Man09, MSCV09, MSC$^+$10, SCH$^+$10, CRS$^+$10, Man11, MCH11, SCH$^+$12, MMCM12, Man12, MTPC12, MCR$^+$13, RMC14, MRM14, MMR$^+$14, MCR$^+$14]
[RR1]	[TPMCM12, MCR$^+$13]
[RR2]	[SCH$^+$12, MTPC12, MRM14, MCR$^+$13]
[RR3]	[MTPC12, MCR$^+$13]
[RR4]	[TPMCM12, MRM14, MCR$^+$13]

representation of complex networks whereby nodes are randomly connected such that the variance in nodal degree is relatively small. They are characterised by a Poisson degree sequence distribution for large number of nodes (n), and the *binomial distribution* for small n.

The Barabási-Albert model [BA99] is related to *scale-free networks*. A scale-free network is a network with degree sequence distribution obeying a power-law form. This is the reason that often, BA-generated networks are also called *power-law networks*. In scale-free networks the topology is such that some vertices, known as hubs, have degrees that are orders of magnitude larger than the average degree.

The Watts and Strogatz (WS) model [WS98] is related to *small-world networks*. The

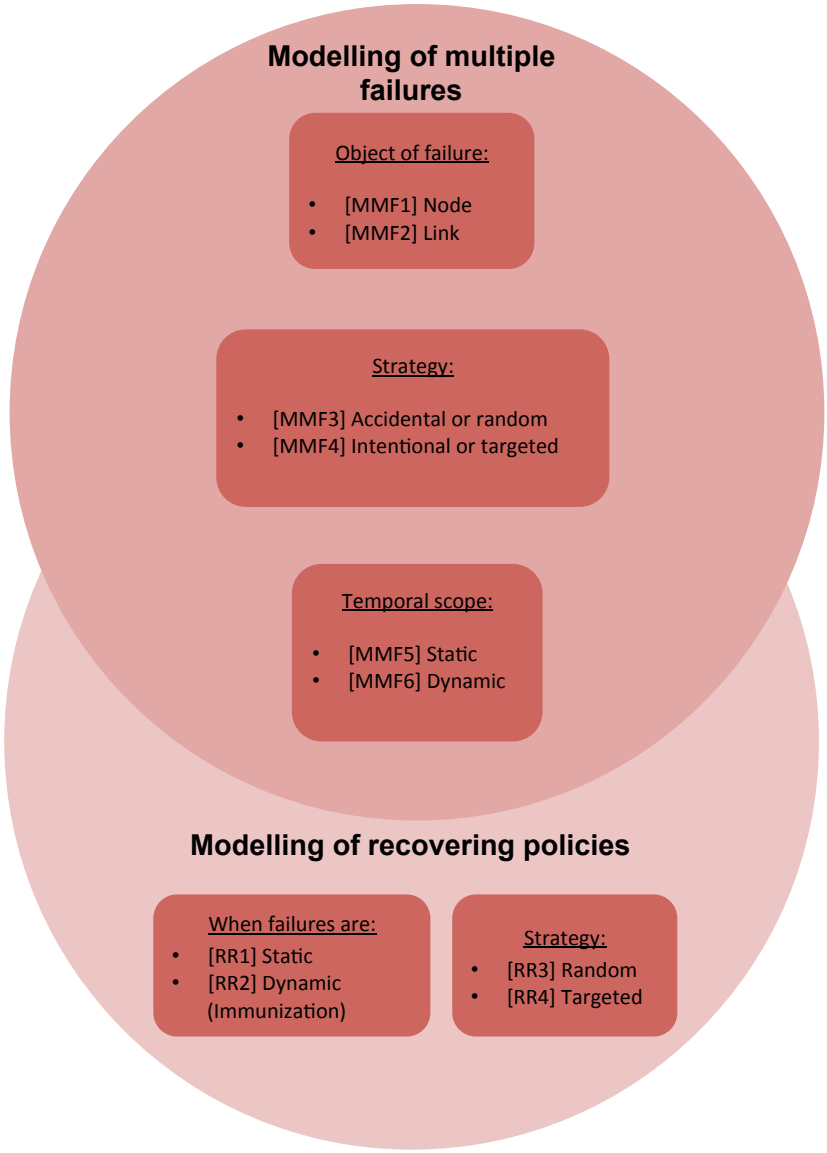


Figure 3.4: Modelling of multiple failures and recovering policies.

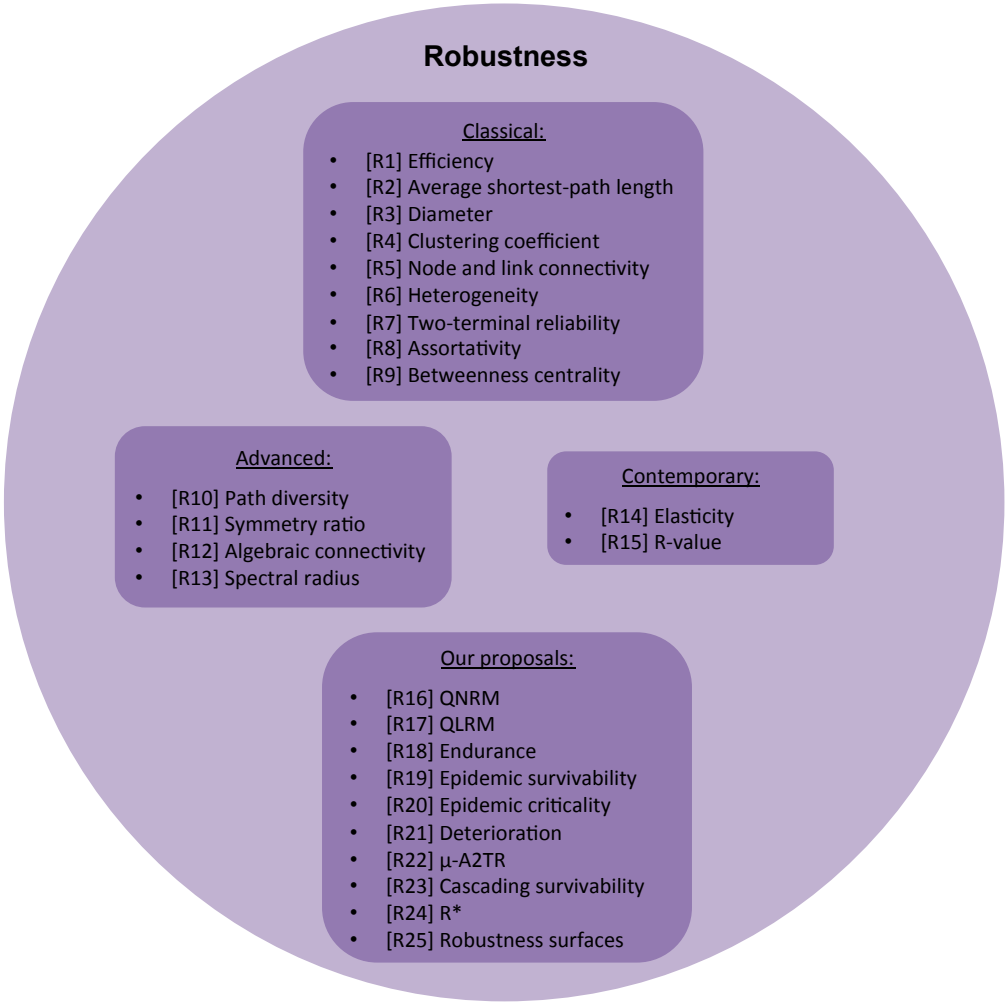


Figure 3.5: Robustness.

term “small-world” comes from the fact that these networks have relatively short average path length, also known as small-world effect [Mie11].

Table 3.2 shows what networks have been considered in each of the articles carried out during this thesis. It can be noted that most of the works have focused on real telecommunication networks (label *CN3*), as well as synthetic networks (labels *CN12*, *CN13* and *CN14*).

The third and fourth blocks are detailed in Fig. 3.4. The *modelling of multiple failures* is divided into three areas: object of failure, strategy and temporal scope. In addition, the *modelling of recovering policies* is partitioned into two areas: the type of the failures (static or dynamic) and the strategy. The relationship between our manuscripts and these two blocs is once more presented in Table 3.3. It is interesting to indicate that most of our works have been focused on node failures, and that the modelling of

Table 3.4: A. Articles that have covered topics of *Robustness*: classical, advanced and contemporary.

Subtopics	Articles
[R1]	[MSS+14b]
[R2]	[CRS+10, Man11, MCH11, TPMCM12, MMCM12, CMM12, CMM12, Man12, MTPC12, MCR+13, BMC+13, BMK+13, MBCK13, MCTP+13, TMCM13, MSS+14b, MCR+14]
[R3]	[Man09, MSCV09, MSC+10, CRS+10, Man11, MCH11, TPMCM12, MMCM12, CMM12, Man12, MTPC12, BMC+13, BMK+13, MBCK13, MCTP+13, TMCM13, MSS+14b]
[R4]	[Man11, MCH11, MMCM12, CMM12, Man12, MTPC12, MCR+13, BMK+13, MBCK13, MCTP+13, MSS+14b, MCR+14]
[R5]	[Man11, MCH11, MMCM12, CMM12, Man12, MTPC12, BMK+13, MBCK13, MCTP+13, MSS+14b]
[R6]	[Man11, MCH11, MMCM12, CMM12, Man12, MTPC12, BMK+13, MBCK13, MCTP+13, MSS+14b]
[R7]	[Man11, MCH11, MSCM12, MMCM12, CMM12, Man12, MTPC12, BMK+13, MBCK13, MCTP+13, MSS+14b]
[R8]	[Man11, MCH11, TPMCM12, MMCM12, CMM12, Man12, MTPC12, MCR+13, BMK+13, MBCK13, MCTP+13, TMCM13, MSS+14b, MCR+14]
[R9]	[TPMCM12, MSCM12, MMCM12, CMM12, Man12, MTPC12, MCR+13, BMK+13, MBCK13, MCTP+13, TMCM13, MSS+14a, MSS+14b, MCR+14]
[R10]	[MSS+14b]
[R11]	[Man11, MCH11, MMCM12, CMM12, Man12, BMK+13, MCTP+13, MSS+14b]
[R12]	[Man11, MCH11, MMCM12, CMM12, Man12, MTPC12, MCR+13, BMC+13, BMK+13, MBCK13, MCTP+13, MSS+14b, MCR+14]
[R13]	[CRS+10, Man11, MCH11, MMCM12, CMM12, Man12, MTPC12, MCR+13, BMC+13, RMC14, BMK+13, MBCK13, MCTP+13, MSS+14b, MCR+14]
[R14]	[CMM12, Man12, MCTP+13, MSS+14a, MSS+14b]
[R15]	[CMM12, Man12, MCTP+13, MSS+14a, MSS+14b]

Table 3.5: B. Articles that have covered topics of *Robustness*: our proposals

Subtopics	Articles
[R16]	[Man11, MCH11, MMCM12, CMM12]
[R17]	[Man11, MCH11, MMCM12, CMM12]
[R18]	[Man12, MCTP$^+$13, MSS$^+$14b]
[R19]	[MCR$^+$13, MCR$^+$14]
[R20]	[MCR$^+$13]
[R21]	[BMC$^+$13, BMK$^+$13]
[R22]	[MBCK13]
[R23]	[MCR$^+$14]
[R24]	[MSS$^+$14a, MSS$^+$14b]
[R25]	[MSS$^+$14a, MSS$^+$14b]

recovering policies has been less addressed than the one of multiple failures.

Finally, the fifth and most important block is presented in Fig. 3.5, which is related to the *network robustness*. As observed, we present the traditional classification of robustness metrics: classical, advanced and contemporary. In addition, *our proposals* area is entirely dedicated to list the ten different robustness metrics that have been presented in this thesis. Tables 3.4 and 3.5 present what metrics have been considered in each of our manuscripts. It is worth noting that we have considered almost uniformly the available robustness metrics in the literature.

3.2 Tools

The tools that have been used in this thesis are detailed below:

- PHISON: A discrete-event network simulator that has been developed in collaboration with Dr. Juan Segovia. PHISON is written in Java and its purpose is to facilitate the study of diverse phenomena related with complex networks. It allows the user to analyse the topological structure of networks, study dynamical aspects of such networks, and evaluate the effects that failures might cause on the services provided by such networks. At the moment there is only one service considered by PHISON, *connections*, which are path-oriented communications between network nodes. It can be found in http://bcds.udg.edu/phison.
- R: A free software programming language, which is widely used for developing statistical software and data analysis. The *igraph* for R library has been used in

order to generate synthetic complex networks, as well as to plot several of the results of the articles outlined in the previous section.

- Matlab: A computing environment that allows matrix manipulations, plotting functions and numerical computing. It has been widely used for the whole period of the thesis in order to generate numerical results, as well as to carry out complex mathematical operations.

- Perl: A scripting language that has been used in order to parse large amounts of results that were generated by PHISON.

- LaTeX: A high-quality document preparation system. It is extensively used to write and publish scientific documents in many fields. It uses a TeX typesetting program for formatting the output. LaTeX has been used as the primarily tool to write the manuscripts presented in this thesis.

3.3 Contributors

It is well-known that knowledge sharing plays a pivotal role in the research field. By teaming up it is possible to conquer frontiers that would have never been imagined. "*L'union fait la force*" (unity makes strength) has been the *leitmotif* of this thesis. Being able to collaborate with different universities has been of inestimable value for the progress of this thesis.

In Fig. 3.6 the set of the contributors with whom we have worked jointly is presented. Besides the supervisor of this thesis (Eusebi Calle, on the top left), this work has co-authored papers with 23 researchers, from 11 different countries, who conduct their professional career in 9 different research institutions. Not counting University of Girona, University Carlos III of Madrid (Spain) has provided the largest number of collaborators, 6. In second place we find Kansas State University, with 3. Then the University of Zagreb (Croatia), North Dakota State University (USA) and the Technical University of Denmark (Denmark) come with 2 co-authors. Lastly, we have teamed up with one researcher of Strathclyde University (Scotland), Raytheon BBN Technologies (USA) and University of Sydney (Australia), respectively.

At the time this thesis is being written, some of the co-authors that were still PhD candidates while we were collaborating, have already defended their PhD. Therefore, it can be said that the full list of partners of this thesis is composed of PhDs and Professors.

To conclude, it is worth noting that it is not trivial to collaborate with foreign research

institutions. Differences in time zones are the most difficult drawback to overcome. In any case, at the end the result is extremely satisfying, and it helps to gather insight and experience in how to work with heterogeneous teams.

 Figure 3.6: Set of contributors that have co-authored papers of the thesis.

Part II Contributions

4 Endurance: a new robustness measure for complex networks under multiple failure scenarios

M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, D. Harle. *Endurance: a new robustness measure for complex networks under multiple failure scenarios.* **Computer Networks**, Volume 57, Issue 17, Pages 3641-3653. (2013).

4.1 Abstract

Society is now, more than ever, highly dependent on the large-scale networks that underpin its functions. In relatively recent times, significant failures have occurred on large-scale networks that have a considerable impact upon sizable proportions of the world's inhabitants. The failure of infrastructure has, in turn, begot a subsequent loss of services supported by that network. Consequently, it is now vitally important to evaluate the robustness of such networks in terms of the services supported by the network in question. Evaluating network robustness is integral to service provisioning and thus any network should include explicit indication of the impact upon service performance. Traditionally, network robustness metrics focused solely on topological characteristics, although some new approaches have considered, to a degree, the services supported by such networks. Several shortcomings of these new metrics have been identified. With the purpose of solving the drawbacks of these metrics, this paper presents a new measure called endurance, which quantifies the level of robustness supported by a specific topology under different types of multiple failure scenarios, giving higher importance to perturbations affecting low percentages of elements of a network. In this paper, endurance of six synthetic complex networks is computed for a range of defined multiple failure scenarios, taking into account the connection requests that cannot be satisfied. It is demonstrated that our proposal is able to quantify the robustness of a network under given multiple failure scenarios. Finally, results show that different types of networks react differently depending on the type of multiple failure.

M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, D. Harle. *Endurance: a new robustness measure for complex networks under multiple failure scenarios*. **Computer Networks**, Volume 57, Issue 17, Pages 3641-3653. (2013)

Received 6 July 2012, Revised 19 July 2013, Accepted 17 August 2013, Available online 24 August 2013

doi:10.1016/j.comnet.2013.08.011

http://www.sciencedirect.com/science/article/pii/S1389128613002740

Abstract

Society is now, more than ever, highly dependent on the large-scale networks that underpin its functions. In relatively recent times, significant failures have occurred on large-scale networks that have a considerable impact upon sizable proportions of the world's inhabitants. The failure of infrastructure has, in turn, begot a subsequent loss of services supported by that network. Consequently, it is now vitally important to evaluate the robustness of such networks in terms of the services supported by the network in question. Evaluating network robustness is integral to service provisioning and thus any network should include explicit indication of the impact upon service performance. Traditionally, network robustness metrics focused solely on topological characteristics, although some new approaches have considered, to a degree, the services supported by such networks. Several shortcomings of these new metrics have been identified. With the purpose of solving the drawbacks of these metrics, this paper presents a new measure called *endurance*, which quantifies the level of robustness supported by a specific topology under different types of multiple failure scenarios, giving higher importance to perturbations affecting low percentages of elements of a network. In this paper, *endurance* of six synthetic complex networks is computed for a range of defined multiple failure scenarios, taking into account the connection requests that cannot be satisfied. It is demonstrated that our proposal is able to quantify the robustness of a network under given multiple failure scenarios. Finally, results show that different types of networks react differently depending on the type of multiple failure.

Keywords

- Robustness; Complex networks; Multiple failures

5 On the Connectivity of Data Center Networks

M. Manzano, K. Bilal, E. Calle, S. U. Khan. *On the Connectivity of Data Center Network*s. **IEEE Communications Letters**, Volume 17, Issue 11, Pages 2172-2175. (2013).

5.1 Abstract

Data Center Networks (DCNs) constitute the communication backbone for the cloud computing paradigm. Recently, network connectivity analysis in terms of reliability has received attention from the network research community. The traditional network features are useful; however, they are insufficient to determine how well-connected or well-designed a DCN is against the node or link removals. In this letter, we present a connectivity analysis of three well-known DCN architectures, namely: (a) ThreeTier, (b) FatTree, and (c) DCell. Our analysis reveals that the classic connectivity measures are inadequate for evaluating DCN connectivity. Therefore, we propose μ-A2TR, a novel metric to characterize network connectivity in the case of node or link failures. Experimental results reveal that the DCNs exhibit a moderate level of connectivity in the case of random node removals. However, connectivity decays abruptly when considering the targeted nodes removal. Moreover, the connectivity analysis depicts significant differences among the considered DCNs.

M. Manzano, K. Bilal, E. Calle, S. U. Khan. *On the Connectivity of Data Center Networks*.
IEEE Communications Letters, Volume 17, Issue 11, Pages 2172-2175. (2013)

Date of Publication : 26 setembre 2013
Date of Current Version : 25 novembre 2013
Issue Date : November 2013

http://dx.doi.org/10.1109/LCOMM.2013.091913.131176

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6612762

Abstract

Data Center Networks (DCNs) constitute the communication backbone for the cloud computing paradigm. Recently, network connectivity analysis in terms of reliability has received attention from the network research community. The traditional network features are useful; however, they are insufficient to determine how well-connected or well-designed a DCN is against the node or link removals. In this letter, we present a connectivity analysis of three well-known DCN architectures, namely: (a) ThreeTier, (b) FatTree, and (c) DCell. Our analysis reveals that the classic connectivity measures are inadequate for evaluating DCN connectivity. Therefore, we propose μ-A2TR, a novel metric to characterize network connectivity in the case of node or link failures. Experimental results reveal that the DCNs exhibit a moderate level of connectivity in the case of random node removals. However, connectivity decays abruptly when considering the targeted nodes removal. Moreover, the connectivity analysis depicts significant differences among the considered DCNs.

Keywords

- Cloud computin; Connectivity analysis; Data center networks; Distributed systems

6 Unveiling Potential Failure Propagation Scenarios in Core Transport Networks

Marc Manzano, Anna Manolova Fagertun, Sarah Ruepp, Eusebi Calle, Caterina Scoglio, Ali Sydney, Antonio de la Oliva, Alfonso Muñoz. *Unveiling Potential Failure Propagation Scenarios in Core Transport Networks.* Submitted to the IEEE Communications Magazine. (2014).

6.1 Abstract

The contemporary society has become more dependent on telecommunication networks. Novel services and technologies supported by such networks, such as cloud computing or e-Health, hold a vital role in modern day living. Large-scale failures are prone to occur, thus being a constant threat to business organizations and individuals. To the best of our knowledge, there are no publicly available reports regarding failure propagation in core transport networks. Furthermore, Software Defined Networking (SDN) is becoming more prevalent in our society and we can envision more SDN-controlled Backbone Transport Networks (BTNs) in the future. For this reason, we investigate the main motivations that could lead to epidemic-like failures in BTNs and SDNTNs. To do so, we enlist the expertise of several research groups with significant background in epidemics, network resiliency, and security. In addition, we consider the experiences of three network providers. Our results illustrate that Dynamic Transport Networks (DTNs) are prone to epidemic-like failures. Moreover, we propose different situations in which a failure can propagate in SDNTNs. We believe that the key findings will aid network engineers and the scientific community to predict this type of disastrous failure scenario and plan adequate survivability strategies.

Marc Manzano, Anna Manolova Fagertun, Sarah Ruepp, Eusebi Calle, Caterina Scoglio, Ali Sydney, Antonio de la Oliva, and Alfonso Muñoz. “Unveiling Potential Failure Propagation Scenarios in Core Transport Networks”. Submitted to *IEEE Communications Magazine*. (2014)

http://arxiv.org/abs/1402.2680

Abstract

The contemporary society has become more dependent on telecommunication networks. Novel services and technologies supported by such networks, such as cloud computing or e-Health, hold a vital role in modern day living. Large-scale failures are prone to occur, thus being a constant threat to business organizations and individuals. To the best of our knowledge, there are no publicly available reports regarding failure propagation in core transport networks. Furthermore, Software Defined Networking (SDN) is becoming more prevalent in our society and we can envision more SDN-controlled Backbone Transport Networks (BTNs) in the future. For this reason, we investigate the main motivations that could lead to epidemic-like failures in BTNs and SDNTNs. To do so, we enlist the expertise of several research groups with significant background in epidemics, network resiliency, and security. In addition, we consider the experiences of three network providers. Our results illustrate that Dynamic Transport Networks (DTNs) are prone to epidemic-like failures. Moreover, we propose different situations in which a failure can propagate in SDNTNs. We believe that the key findings will aid network engineers and the scientific community to predict this type of disastrous failure scenario and plan adequate survivability strategies.

Index Terms

Backbone Transport Networks; SDN-controlled Transport Networks; Failure Propagation; Epidemics.

Main Results and Conclusions Part III

7 Results

This chapter outlines the main results derived from this thesis. All of our contributions target either the modelling of multiple failure scenarios, the study of the robustness of complex networks, and in a less extent, the protection and recovery of network elements under multiple failure scenarios. According to our methodology (see chapter 3), we have been able to constantly increase the complexity of our work. Therefore, the same contribution/proposal can be related to more than one manuscript.

Our modelling of multiple failures contributions are:

1. **A multiple failure taxonomy:** In order to model multiple failures, we required a clear, simple and inclusive multiple failure classification. In [MCH11, MCTP+13], we identified that multiple failure scenarios proposed in the literature can be broadly classified as either random or targeted scenarios. In a random multiple failure case, node and link failures occur as a result of random actions on network elements (e.g., natural disasters). On the contrary, elements in a targeted multiple failure are chosen in order to maximise the impact of such failures and there is an element of discrimination. Additionally, both types of attacks can be either static or dynamic. Static multiple failures are essentially one-off failures that affect one or more elements (nodes or links) simultaneously at any given point. Dynamic failures have a temporal dimension. Epidemic-like or cascading failures are an example of dynamic failures. It is worth noting that there were previous taxonomies, which we enhanced in our proposal in order to consider dynamic multiple failure scenarios.

2. **A novel epidemic model for telecommunication networks:** The problem of epidemics, also referred to as virus spreading or failure propagation, has attracted huge interest among the scientific community. Although there are several families described in the literature dealing with epidemic models, none of

them could be used to model a failure propagation in GMPLS-based networks. Therefore, we extended the SIS model by proposing the *SID epidemic model* [MSCV09, MSC+10, SCH+10, CRS+10, MCH11, SCH+12, MMCM12, MTPC12, MCR+13]. In our model, each node of the network can be in one of three states: susceptible (uninfected), infected, or disabled. The disabled state takes into account the fact that an infected node could degrade to complete nodal failure (i.e., control and data plane failure). When a node becomes disabled, all connections crossing that node are removed. In that case, the node needs a process to be repaired, and the time needed is directly proportional to the MTTR.

3. **Description of possible epidemic-like failure scenarios in telecommunication networks:** We carried out a thorough study in order to identify which situations could lead to epidemic-like failure propagation in BTNs. Moreover, we also considered the future SDNTNs [MMR+14]. This contribution was based on the research carried out *a posteriori* of the presentation of the SID model.

4. **Enhancement of the SID analytical model:** Due to the lack of accuracy that existed between the analytical model predictions of the SID model, and the results obtained from simulations, we introduced a slight modification of the SID model mean-field equations not applied before. As a consequence, we improved the theoretical predictions with respect to stochastic simulations [RMC14]. In addition, the new epidemic threshold that we defined can be generalised to other networks and similar models.

It is interesting to note that the third and fourth contributions are derived from the proposal of the SID epidemic model. Hence, it can be asserted that our contributions complement one another.

Our network robustness contributions are listed below:

1. **Quantitative and Qualitative Robustness Metrics (QNRM and QLRM)**: From the network operator perspective, failures affect the number of established and future connection demands. Considering both aspects (quantity and quality) these two metrics were proposed to evaluate how network services could be affected after different multiple failure scenarios. On one hand, *QLRM* quantifies variations in the average shortest-path length of established connections, reflecting that many key QoS parameters are functions of path length (delays, packet loss, etc.). On the other hand, *QNRM* evaluates the number of blocked connections [MCH11, MMCM12].

2. **Epidemic survivability (ES):** Nowadays, with the increasing computation capacity and complexity of operating systems of modern network devices (routers, switches, etc.), the study of possible epidemic-like failure scenarios has become of paramount importance. When epidemics occur, such as in other multiple failure scenarios, identifying the level of vulnerability offered by a network is one of the main challenges. Therefore, we proposed *epidemic survivability*, a new network measure that describes the vulnerability of each node of a network under a specific epidemic intensity [MCR+13, MCR+14]. This metric was designed according to the SIS (Susceptible-Infected-Susceptible) epidemic model. Moreover, this metric is able to identify the set of nodes which are more vulnerable under an epidemic attack.

3. **Epidemic criticality (EC):** We introduced epidemic criticality, a novel robustness metric suitable for epidemic failure scenarios [MCR+13], which is based on the *ES* network measure.

4. **Endurance:** According to the Oxford dictionary, *endurance* has been used to describe the ability of an organism to withstand an adverse situation in order to remain active for a long period of time. We applied the meaning of *endurance* to the context of a complex network with connections running over it. *Endurance* computes the robustness of a network under multiple failure scenarios given one or more QoS parameters (e.g. delay) or graph metrics (e.g. size of the largest connected component) [MCTP+13]. Furthermore, our proposal gives higher importance to perturbations affecting low percentages of elements of a network. This feature is key when assessing the robustness of networks because such scenarios are more likely to occur.

5. **Deterioration:** In [BMK+13, BMC+13], we observed that depending on the: DCN architecture (physical structure), type of failure (whether it is random or targeted), and specific percentage of the nodes failed, the level of robustness according to a specific graph metric, computed from the largest connected component might be different. Therefore, we proposed the *deterioration* metric, a procedure for the quantification of the DCN robustness based on the percentage change in various graph metrics. The *deterioration* metric can be employed to evaluate the robustness of the networks where the classical robustness metrics are inapplicable, such as the DCNs.

6. **μ-A2TR:** To complement the previous contribution, and given that classic connectivity measures are inadequate for evaluating DCN connectivity, we proposed μ-A2TR, a novel metric to characterise network connectivity in the case of node or link failures [MBCK13].

7. **Cascading survivability (CS):** To fully characterise the dynamic events (e.g. failures) that might happen in complex networks, we also modelled cascading failures. As a consequence, we proposed *cascading survivability*, which characterises how potentially injurious a node is according to a cascading failure scenario [MCR+14]. In fact, *CS* is to cascading failures, what *ES* is to epidemics. Therefore, with these metrics we covered the two main dynamic multiple failure scenarios.

8. ***R****:** Despite the robustness of complex networks has been extensively studied in the last decade, there was still lacking a unifying framework able to embrace all the proposed metrics. In the literature there are two open issues related to this gap: (a) how to dimension several metrics to allow their summation and (b) how to weight each of the metrics. Therefore, we introduced the R^*-value, which extracts the most informative robustness metric for a failure scenario [MSS+14a, MSS+14b]. Given a set of robustness metrics, the R^* provides a single value in the interval [0,+∞]. In addition, besides finding the most informative robustness metric, we adjust the initial robustness to 1, thus simplifying the comparison of network robustness variations when failures occur.

9. **Robustness surfaces (Ω):** To complement the R^*, we proposed the *robustness surfaces*, which allows network robustness variations of different networks to be visually assessed, regardless of the failure scenario [MSS+14a, MSS+14b].

The results related with protection and recovery of network elements are:

1. **Traffic-level community protection:** Large-scale failures in telecommunication networks have been traditionally mitigated by attempting to preserve global connectivity in the network. However, although communication inside communities may be of high relevance, their preservation is a challenging task. By defining a new concept of community, we introduced six novel community-based strategies that, when working within a limited budget, are able to determine which are the best candidate nodes to protect [TPMCM12, TMCM13].

2. **High Epidemic Survivability (HES) and High Epidemic Survivability Adaptive (HESA):** These two immunisation strategies were proposed in [MCR+13], and are based on the *ES* measure. Under epidemic-like failure scenarios, network vulnerability can be significantly reduced by using either of these two proposals, compared to other existing methods.

3. **Vulnerability Score:** In order to propose several strategies for cost-effective network performance improvement via differentiated repair times, we proposed

the *vulnerability score*, which indicates how many times (on average) a node is hit by an epidemic spreading (i.e. performs transition from the susceptible to the infected state), given a specific epidemic scenario [MRM14].

Besides, although we have not based any of our contributions on complex networks, several well-known theoretical models have been thoroughly studied. Their robustness under multiple failure scenarios has been evaluated. Moreover, for instance, we have identified which of these models represents more accurately specific types of real networks. Finally, we have also proposed a multilayered graph model of the main DCN architectures.

8 Conclusions and Future Work

The aim of this thesis was to investigate, propose and validate new robustness evaluation mechanisms for complex networks. The main contributions of this work, which are strongly related with the objectives that were defined (see chapter 2), are summarised next:

1. **Robustness metrics:** we have proposed several robustness metrics, which have been shown to be suitable to evaluate the network robustness under a wide range of multiple failure situations. Besides, we have also presented a unifying framework to visually assess the network robustness while considering several robustness metrics.

2. **Modelling of multiple failures:** firstly we defined a multiple failure taxonomy, that, secondly, allowed us to model several multiple failure scenarios. For instance, we have considered random and targeted static failures, and epidemic-like and cascading failures.

3. **PHISON:** In collaboration with Dr. Juan Segovia, we designed and implemented our own discrete-event network simulator. The different modules that now comprise PHISON have been added incrementally, according to the needs that were arising during this work.

Not all the robustness metrics that we have proposed can be used to evaluate the goodness of a network under each of the multiple failure scenarios that we have considered. Depending on the underlying requirements that arise in order to compute a robustness metric, it can be applied to either (a) any (e.g., endurance or R^*), (b) static (e.g., deterioration or μ-A2TR) or (c) dynamic (e.g., epidemic criticality) multiple failure scenarios.

Regarding the last objective of this thesis,"*present a categorization of the different robustness degrees that distinct complex networks have*", it is worth noting that it has not been possible to define such classification. The reason has been discussed in [MSS+14b]: there is no universal metric able to quantify the network robustness. We have found out that the network robustness varies depending on:

- The multiple failure scenario.
- The network that is under study.
- The set of considered metrics.

Therefore, *the network robustness* totally depends on the field or situation in which the study is done. For instance, a telecommunication networks operator might consider a set of metrics (e.g., jitter, delay, lost connections) to compute the R^*, while a power grid engineer could possibly consider different metrics.

Finally, there are several issues that have been left for future work:

- The extension of *endurance* in order to allow more than one robustness metric or Quality of Service (QoS) parameter as input.
- The re-definition of the *epidemic survivability* measure for the SID epidemic model.
- A thorough investigation of which robustness metrics are more effective in order to quantify the network robustness via R^* of a specific type of network.
- A study of the scalability of the robustness surfaces (Ω) with respect to the network size.
- A proposal of a network robustness refinement methodology, based on the robustness surfaces (Ω).
- An investigation on whether there are other possible fields were our contributions could be applied. For instance, to characterise water distribution networks or interdependent networks.

Appendix Part IV

A Rest of journal publications

E. Calle, J. Ripoll, J. Segovia, P. Vilà, and M. Manzano. *A múltiple failure propagation model in GMPLS-based networks*. **IEEE Network**, Volume 24, Issue 6, Pages 17-22. (2010)

Date of Publication : November-December 2010
Date of Current Version : 11 novembre 2010
Issue Date : November-December 2010

http://dx.doi.org/10.1109/MNET.2010.5634438

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5634438

Abstract

In this article, a new model to simulate different failure propagation scenarios in GMPLS-based networks is proposed. Several types of failures and malfunctions may spread along the network following different patterns (hardware failures, natural disasters, accidents, configuration errors, viruses, software bugs, etc.). The current literature presents several models for the spreading of failures in general networks. In communication networks, a failure affects not only nodes but also the connections passing through those nodes. The model in this article takes into account GMPLS node failures, affecting both data and control planes. The model is tested by simulation using different types of network topologies. In addition, a new method for the classification of network robustness is also introduced**.**

Keywords

- GMPLS node failure
- GMPLS-based network
- communication network
- multiple failure propagation model
- network robustness
- network topology

I Seoane, E. Calle, J. A. Hernández, J. Segovia, R. Romeral, P. , M. Urueña and M. Manzano. *Failure propagation in GMPLS optical rings: CTMC model and perfomance analysis.* **Optical switching and networking**, Volume 9, Issue 1, Pages 39-51. (2012)

Received 22 October 2010, Revised 17 March 2011, Accepted 25 April 2011, Available online 19 May 2011

http://dx.doi.org/10.1016/j.osn.2011.04.002

http://www.sciencedirect.com/science/article/pii/S1573427711000269?np=y

Abstract

Network reliability and resilience has become a key design parameter for network operators and Internet service providers. These often seek ways to have their networks fully operational for at least 99.999% of the time, regardless of the number and type of failures that may occur in their networks.

This article presents a continuous-time Markov chain model to characterise the propagation of failures in optical GMPLS rings. Two types of failures are considered depending on whether they affect only the control plane, or both the control and data planes of the node. Additionally, it is assumed that control failures propagate along the ring infecting neighbouring nodes, as stated by the Susceptible-Infected-Disabled (SID) propagation model taken from epidemic-based propagation models. A few numerical examples are performed to demonstrate that the CTMC model provides a set of guidelines for selecting the appropriate repair rates in order to attain specific availability requirements, both in the control plane and the data plane.

Keywords

- Optical GMPLS rings; Epidemic propagation of errors; Continuous-time Markov chains; Reliability analysis

K. Bilal, M. Manzano, S. U. Khan, E. Calles, Keqin Li, and A. Y. Zomaya. *On the characterization of the estructural robustness of data centre networks.* **IEEE transactions on cloud computing.** Volume 1, Issue 1, Pages 1-1. (2013)

Date of Publication : 19 setembre 2013
Date of Current Version : 25 novembre 2013
Issue Date : Jan.-June 2013

http://dx.doi.org/10.1109/TCC.2013.6

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6604388

Abstract

Data centers being an architectural and functional block of cloud computing are integral to the Information and Communication Technology (ICT) sector. Cloud computing is rigorously utilized by various domains, such as agriculture, nuclear science, smart grids, healthcare, and search engines for research, data storage, and analysis. A Data Center Network (DCN) constitutes the communicational backbone of a data center, ascertaining the performance boundaries for cloud infrastructure. The DCN needs to be robust to failures and uncertainties to deliver the required Quality of Service (QoS) level and satisfy Service Level Agreement (SLA). In this paper, we analyze robustness of the state-of-the-art DCNs. Our major contributions are: (a) we present multi-layered graph modeling of various DCNs; (b) we study the classical robustness metrics considering various failure scenarios to perform a comparative analysis; (c) we present the inadequacy of the classical network robustness metrics to appropriately evaluate the DCN robustness; and (d) we propose new procedures to quantify the DCN robustness. Currently, there is no detailed study available centering the DCN robustness. Therefore, we believe that this study will lay a firm foundation for the future DCN robustness research.

Keywords

- Cloud computing Computer architecture Data processing Information technology
- Network topology Quality of service Servers

V. Torres-Padrosa, M- Manzano, E. Calle, and M. Manzano. *Community-based traffic preservation in telecommunications networks.* **International Journal of Communication Systems.** (2013)

This publication is a follow-up of the research presented in the paper 'Traffic-level Community Protection in Telecommunication Networks under Large-Scale Failures' in SPECTS 2012 conference.

Article first published online: 2 DEC 2013

http://dx.doi.org/10.1002/dac.2702

http://onlinelibrary.wiley.com/doi/10.1002/dac.2702/full

Abstract

Large-scale failures in telecommunication networks have been traditionally mitigated by attempting to preserve global connectivity in the network. However, although communication inside communities may be of high relevance, their preservation is a challenging task. To achieve this, we propose a new concept of community that combines not only the topological information of the network but also the traffic-level interaction. This new concept is then used to present six novel community-based strategies that, when working within a limited budget, are able to determine which are the best candidate nodes to protect. The strategies proposed have been tested over four different types of networks and have been compared with other well-known immunization or protection methods. Results show that community-based strategies better preserve the inner community traffic with respect to traditional approaches. Furthermore, in some cases, both global and intra-community traffic preservation is able to be improved.

Keywords

- complex networks;
- communities;
- large-scale failures;
- telecommunication networks;
- network protection

K. Bilal, M. Manzano, S. U. Khan, E. Calles, Keqin Li, and A. Y. Zomaya. *Dissecting the protocol and network traffic of the OnLive cloud gaming platform.* **IEEE transactions on cloud computing.** Volume 20, Issue 5, Pages 451-470. (2014)

Date: 28 Mar 2014

http://dx.doi.org/10.1007/s00530-014-0370-4

http://link.springer.com/article/10.1007%2Fs00530-014-0370-4

Abstract

Cloud gaming is a new paradigm that is envisaged to play a pivotal role in the video game industry in forthcoming years. Cloud gaming, or gaming on demand, is a type of online gaming that allows on-demand streaming of game content onto non-specialised devices (e.g. PC, smart TV, etc.). This approach requires no downloads or game installation because the actual game is executed on the game company's server and is streamed directly to the client. Nonetheless, this revolutionary approach significantly affects the network load generated by online games. As cloud gaming presents new challenges for both network engineers and the research community, both groups need to be fully conversant with these new cloud gaming platforms. The purpose of this paper is to investigate OnLive, one of the most popular cloud gaming platforms. Our key contributions are: (a) a review of the state-of-the-art of cloud gaming; (b) reverse engineering of the OnLive protocol; and (c) a synthetic traffic model for OnLive.

Keywords

- Cloud gaming
- Online games
- OnLive
- Protocol
- Reverse engineering
- Traffic modelling

Spread of epidemic-like failures in telecommunication networks

J. Ripoll[a,1], M. Manzano[b], E. Calle[b]

[a] *Department of Computer Science, Applied Mathematics and Statistics, University of Girona, Spain*
[b] *Department of Architecture and Computers Technology, University of Girona, Spain*

Abstract

We study epidemic-like failures in telecommunication networks. A mean-field model taking two levels of failure into account is introduced where infection, recovery and transition rates are node/link specific. Regarding the short-term epidemic outbreak, an epidemic threshold is stated in terms of the basic reproduction number computed as the largest eigenvalue of a weighted adjacency matrix of the network. As to the long-term endemic situation, we have proved the existence and uniqueness of a steady state. We check the accuracy of the model by means of Monte Carlo simulations. To improve the level of accuracy, we propose a slight modification of the mean-field equations which changes the way we compute the probability for a node of acquiring the infection from one of its neighbors. As a consequence, correlations between probabilities of different states are implicitly incorporated into the model giving improved predictions and being very close to simulation-based data.

Keywords: Epidemic network models; Mean-field theory; Basic reproduction number; Steady states; Stochastic simulations.

1. Introduction

Human history has been related to epidemics, being many civilizations ravaged by epidemic outbreaks such as the Influenza pandemic in 1918, or the 2009 new flu strain H1N1 that hit the world leading a pandemic with a large amount of infections and panic. As a consequence, the analysis and the use of epidemic models have drawn the attention of many researchers of different fields. Realistic epidemic models take some spatial heterogeneity into account that can be incorporated through the network of contacts for instance [1], [2], [3]. Although epidemic models were originally developed targeting biological populations/networks [4], nowadays they are widely used in other contexts such us the spread of rumours/opinions on social networks, the spread of digital viruses on communication infrastructures, etc.

In our high-tech society, people have become more and more dependent on communication networks, either for business or leisure purposes. Moreover, this dependency is expected to grow considering the myriad

Email addresses: jripoll@imae.udg.edu (J. Ripoll), mmanzano@eia.udg.edu (M. Manzano), eusebi@eia.udg.edu (E. Calle)
[1] Phone number: (0034) 972 41 84 14. Fax number: (0034) 972 41 87 92

A. Manolova Fagertun, S. Ruepp, and M. *Resolving epidemic network failures through differentiated repair times.* **IET Networks.** Volume 4, Issue 1, Pages 65-73. (2015)

Received on 17th July 2013

Revised on 11th December 2013

Accepted on 10th April 2014

http://dx.doi.org/10.1049/iet-net.2013.0102

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6994371

Abstract

In this study, the authors investigate epidemic failure spreading in large-scale transport networks under generalised multi-protocol label switching control plane. By evaluating the effect of the epidemic failure spreading on the network, they design several strategies for cost-effective network performance improvement via differentiated repair times. First, they identify the most vulnerable and the most strategic nodes in the network. Then, via extensive event-driven simulations they show that strategic placement of resources for improved failure recovery has better performance than randomly assigning lower repair times among the network nodes. They believe that the event-driven simulation model can be highly beneficial for network providers, since it could be used during the network planning process for facilitating cost-effective network survivability design.

Keywords

Optical fibre networks; Communication switching; Protocols; Reliability; Multiplexing and switching in optical communication; Communication network design, planning and routing

B Submitted articles (available in the arXiv)

Robustness surfaces of complex networks

Marc Manzano[1,†,‡], Faryad Sahneh[2], Caterina Scoglio[2],
Eusebi Calle[1], Jose Luis Marzo[1,2]

[1]*Department of Architecture and Computers Technology, University of Girona, Spain*
[2]*Department of Electrical and Computer Engineering, Kansas State University, USA*

Abstract

Despite the robustness of complex networks has been extensively studied in the last decade, there still lacks a unifying framework able to embrace all the proposed metrics. In the literature there are two open issues related to this gap: (a) how to dimension several metrics to allow their summation and (b) how to weight each of the metrics. In this work we propose a solution for the two aforementioned problems by defining the R^*-value and introducing the concept of *robustness surface* (Ω). The rationale of our proposal is to make use of Principal Component Analysis (PCA). We firstly adjust to 1 the initial robustness of a network. Secondly, we find the most informative robustness metric under a specific failure scenario. Then, we repeat the process for several percentage of failures and different realizations of the failure process. Lastly, we join these values to form the robustness surface, which allows the visual assessment of network robustness variability. Results show that a network presents different robustness surfaces (i.e., dissimilar shapes) depending on the failure scenario and the set of metrics. In addition, the robustness surface allows the robustness of different networks to be compared.

The study of complex networks has attracted significant attention in the past decade. Critical infrastructures such as power grids, telecommunication networks or transportation networks, among others, are complex networks which are omnipresent and play a pivotal role in ensuring the smooth functioning of modern day living. These networks have to constantly deal with failures of their components, hence, any disruption of the service provided might have a considerable impact upon sizable proportions of the world's inhabitants. Thus, understanding not only the structure, but also the dynamics of such networks is of paramount importance.

Failures can be classified as being either random (i.e., accidental) or intentional (also referred to as targeted or deliberated) [1,2]. Accidental failures occur as a result of random actions on network elements (e.g., human-made errors or natural disasters). In contrast, in intentional attacks components are chosen according to some criterion in order to maximize the impact of the failures (e.g., a Denial-of-Service (DoS) attack). We define a *failure scenario* as the pair given by a specific type of failure (e.g., node or link) and a given attack strategy (e.g., random or intentional).

For network engineers and operators it is crucial to quantify the tolerance of a network to a given failure scenario. Robustness is defined as the ability of a network to maintain its total throughput under node or link removal [3, 4].

Robustness metrics have been evolving since the advent of network science. Initially, several works studied the robustness of complex networks by considering a single graph metric: efficiency [5], average shortest-path length [6, 7], diameter [8], clustering coefficient [6, 9], node and link connectivity [10], heterogeneity [11], two-terminal reliability [12], assortativity [13], betweenness centrality [14], among

[†]mmanzano@eia.udg.edu
[‡]This work was done while visiting the EPICENTER research group at Kansas State University, USA.

others. Later on, new metrics were proposed in order to capture advanced characteristics (i.e., by means of spectral graph theory): symmetry ratio [15], algebraic connectivity [16] or spectral radius [17]. Furthermore, other works presented more contemporary metrics which were based on classical graph features. For instance, the authors of [18] studied the robustness in terms of flow diversity, a metric based on the shortest-path length. More recently, generic procedures to capture the robustness of a network for the whole spectrum of possible failures have been presented. Metrics such as elasticity [3] or endurance [2] quantify the robustness of a network according to a single throughput parameter. Trajanovski et al., have proposed a framework to evaluate the robustness of complex networks, which is based on the generic metric R-value [19]. From now on, we will use the conventions defined in Table 1. According to [20], the R-value is denoted by:

$$R = \sum_{k=1}^{n} s_k t_k \tag{1}$$

where s and t are $n \times 1$ weight and graph metric vectors, respectively, and n is the number of robustness metrics. Thus, the R-value includes several graph metrics characterizing network robustness. However, there are two open issues related to the normalization of the t metrics:

1. How to unify the dimensionality of each robustness metric of vector t in order to legitimate their summation.
2. How to define the weight of each metric to optimally extract the most significant information.

In this work we propose a solution for the two aforementioned problems by defining the R^*-value and introducing the concept of *robustness surface* (Ω). The former extracts the most informative robustness metric for a failure scenario, while the latter allows network robustness variations of different networks to be visually assessed, regardless of the failure scenario.

Results

R^*-value. The rationale of our proposal is to make use of Principal Component Analysis (PCA) (see *Methods*). Given a set of robustness metrics t, we first define the initial robustness as follows:

$$R^*_{init} = \sum_{k=1}^{n} \hat{v_k} t^0_k = 1 \tag{2}$$

where t^0 is the set of metrics when no failures occur, and $\hat{v}$ is a normalized eigenvector or Principal Component (PC). We obtain $\hat{v}$ from the procedure that computes the robustness surface (see following subsection and Eq. 4). The fact that $\hat{v}$ is normalized makes R^*_{init} equal to 1. Additionally, R^* can be computed when $p\%$ of elements fail as denoted next:

$$R^*_p = \sum_{k=1}^{n} \hat{v_k} t^p_k \tag{3}$$

where t^p_k is the set of metrics computed when $p\%$ of failures occur. R^*_p takes values in the interval $[0,+\infty)$.

The difference between R^* and R (Eq. 1) is that in our proposal the principal component $\hat{v}$ gives dimension and non-arbitrary weights to each of the metrics. In addition, besides finding the most informative robustness metric, we adjust the initial robustness to 1, thus simplifying the comparison of network robustness variations when failures occur.

Robustness surface (Ω). The robustness surface allows the network performance variability for a given failure scenario to be visually assessed.

In fact, Ω is a matrix where the rows are the percentage of failures (P) and the columns are the distinct failure configurations (m). The list of percentage of failures P (e.g., $P = \{1\%, 2\%..100\%\}$) denotes the range of failures for which the robustness is evaluated. A *failure configuration* represents a realization of the failure process. The different failure configurations m depict the different subsets of elements that fail for a given percentage of failures, with each subset being distinct from one another. The robustness value in $\Omega[p][i]$, where $p \in \{1\%..|P|\%\}$ and $i \in \{1..m\}$, is given by R^*_p (Eq. 3).

To obtain the robustness surface of a network given a failure scenario (e.g., node and random), we define the following procedure:

1. Let A_p be an $m \times n$ matrix where $p \in \{1\%..|P|\%\}$ is the percentage of failure. The goal is to transform A_p into a smaller data set, i.e., a vector ω_p of size m, while preserving the most significant information. Therefore, we define ω_p as a vector of size $m \times 1$. ω_p contains the set of m values R_p^* computed when $p\%$ of elements fail.

2. To do so, we first compute the covariance matrix C_p of each matrix A_p. Then, we average the $|P|$ covariance matrices to obtain a unique matrix $\bar{C}$. This allows us to obtain a PC independent of p.

3. We calculate the eigenvectors V and the eigenvalues D of $\bar{C}$. At this point, the l most relevant eigenvectors of V are taken as the principal components for each matrix A_p (see *Methods* for further details). Hereafter we assume that $l = 1$, i.e., v is the eigenvector PC.

4. Then, we obtain $\hat{v}$ by normalizing v:

$$\hat{v}_j = \frac{v_j}{\sum_{k=1}^{n} t_k^0 v_k} \qquad j \in \{1..n\} \tag{4}$$

5. By multiplying the principal component $\hat{v}$ by each row of A_p we obtain a vector ω_p of size m. Each value of ω_p is, indeed, R_p^*. Next, by iterating this procedure for all matrices A_p, we obtain a set of $|P|$ vectors ω_p. Finally, we define ω'_p as a vector ω_p sorted in decreasing order. Consequently, the robustness surface is given by the following expression $\Omega = \{\omega'_{1\%}, ..., \omega'_{|P|\%}\}$.

Although different failure scenarios (e.g, link random and link by betweenness centrality) provide different $\hat{v}$, each of them satisfies Eq. 2 because $\hat{v}$ is normalized (as shown in Eq. 4).

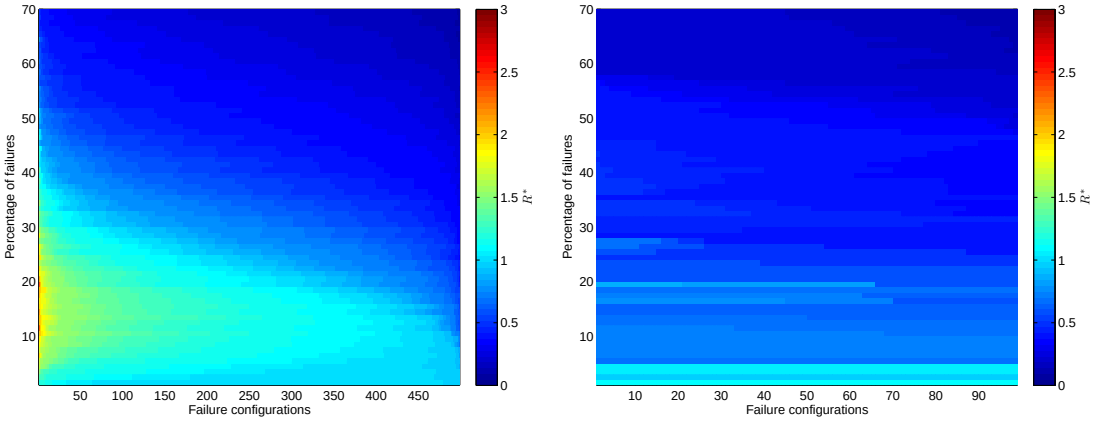
Case study. Here, we illustrate the suitability of our proposal for evaluating the robustness when considering several metrics. To do so, we study two real critical infrastructures: the Spanish railway network (*sprailway*) [21] and the European power grid network (*europg*) [22].

We consider incremental and irreversible random and targeted attacks (e.g., betweenness centrality (BC) or node degree). Link and node failures are considered for the *sprailway* and *europg*, respectively, to show that the robustness surface allows us to compare network robustness independently from the failure scenario. Link failures are caused randomly and by link BC, whereas node failures are caused randomly, by node degree, the clustering coefficient and node BC. In both cases, $|P|$ is set to 70, i.e., from 1% to 70% of failures. The presented results are obtained for 500 and 100 runs (m) for random and targeted attacks, respectively. For each of the runs, a different realization of the failure process is considered, i.e., a distinct subset of elements that fail according to the failure scenario.

We consider the following metrics: the largest connected component (LCC), the degree of fragmentation as a function of the number of connected components (only applicable to link failures), the average nodal degree, the two-terminal reliability, the average clustering coefficient, the average shortest-path length, the diameter, the average node BC, the average link BC and the algebraic connectivity. Therefore, link failures have $n = 10$ while node failures have $n = 9$.

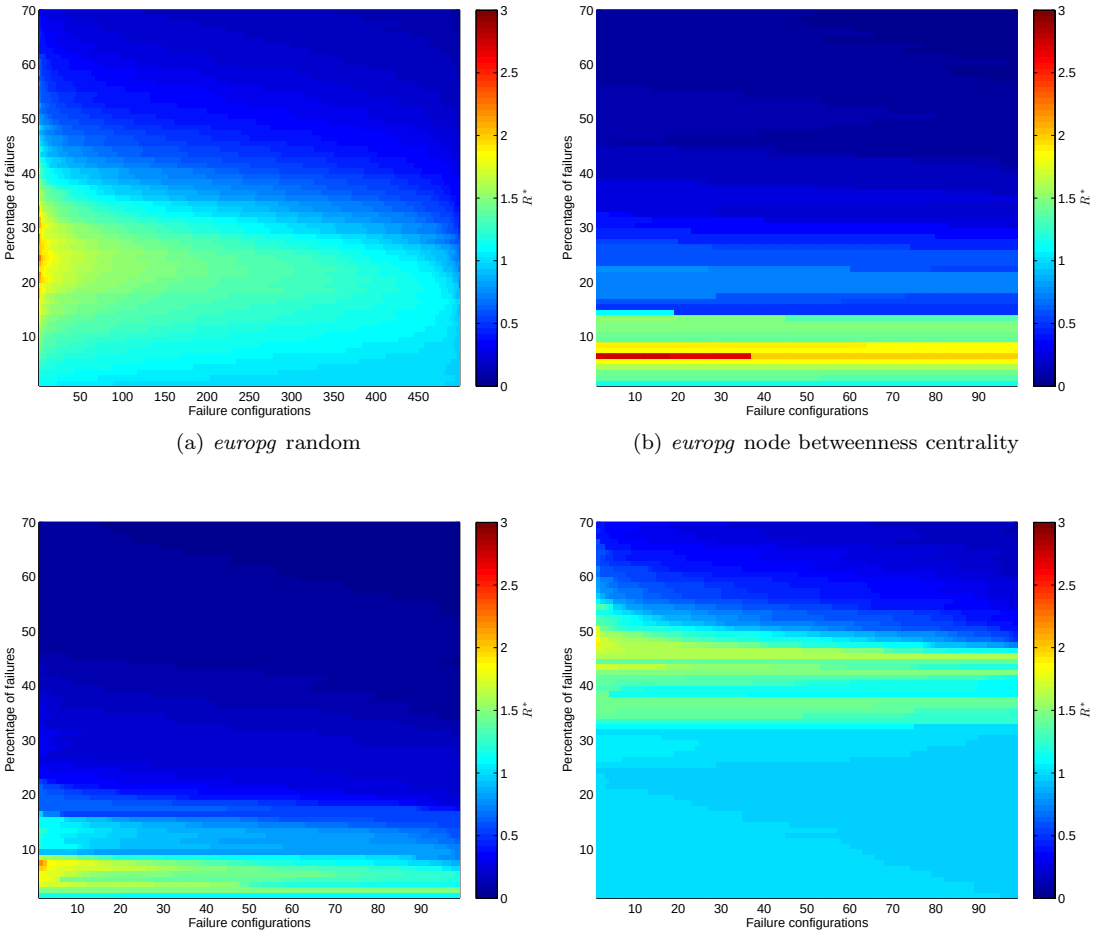
Table 2 presents the main characteristics of the two networks considered. Although both networks have a different number of nodes and links, they show a similar average node degree $\langle k \rangle$, which is between 2 and 3. However, *europg* has a higher node maximum degree, what means that such a network is more vulnerable to targeted attacks. The average shortest-path length $\langle l \rangle$ depicts that *europg* is about two times wider than *sprailway*. Finally, both networks have a negative value of assortativity (r), which means that nodes of dissimilar degrees are connected to each other.

Numerical results. The results of our work are presented in Figures 1 and 2. The x-axes show the different failure configurations for which the n metrics have been computed. The y-axes depict the range of percentage of failures (from 1% to 70%). At each coordinate (x,y), i.e., for each percentage of failures and for each subset of elements that fail, the R_p^*-value is shown. In each figure the range of colors expresses variability, with dark blue and dark red being the two extremes of each failure scenario intervals. Since $R_{init}^* = 1$, i.e., the initial robustness is set to 1 regardless of the set of n chosen metrics, our results allow a visual assessment of the robustness variation with respect to the initial conditions. The further the value of R_p^* is with respect to R_{init}^*, the lower the performance of the network is. When R_p^* is close to 0, the performance is considered to be totally deteriorated. Moreover, it is possible to



(a) *sprailway* random (b) *sprailway* link betweenness centrality

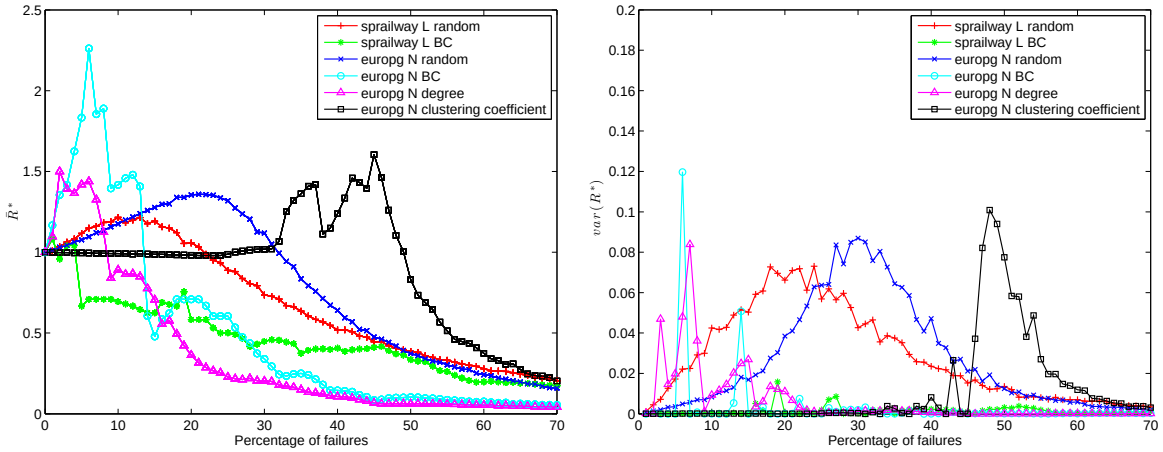
Figure 1: Robustness surface Ω of *sprailway* when causing links to fail randomly and by link BC.



(a) *europg* random (b) *europg* node betweenness centrality

(c) *europg* node degree (d) *europg* node clustering coefficient

Figure 2: Robustness surface Ω of *europg* when causing nodes to fail randomly, by node BC, by node degree and by the clustering coefficient.



(a) Mean: $\bar{R}^*$ (b) Variance: R^*

Figure 3: Robustness summary of *sprailway* and *europg* under the different failure scenarios. As to the legend, L refers to link failures, whereas N refers to nodes.

observe $R^*_p = 1$ when $p \geq 1\%$, and the LCC of the network has similar properties to the initial network (without failures).

Figure 1 presents the robustness surface Ω of *sprailway* in the case of random (Fig.1a) and link BC failures (Fig.1b). Interestingly, the random case provides a smooth surface, while the targeted case presents abrupt slopes. The latter is worth noting, because the presence of abrupt slopes in the robustness surface means that there are network elements (in this case, links) that could be protected in order to improve the overall network robustness.

In the case of *europg*, Fig. 2 depicts four robustness surfaces under different node failure scenarios. Similar to *sprailway*, the random surface depicts a regular behavior. In addition, the targeted-based cases depict rough surfaces. While Figs. 2b and 2c depict that *europg* is not robust under node degree or node BC failure scenarios, Fig. 2d shows that the network keeps the initial robustness until more than 30% of the nodes have failed. This implies that *europg* is significantly more robust under failures by the clustering coefficient than by other targeted strategies.

For some failure configurations, it is worth noting that R^*_p might increase at some percentage of failures with respect to R^*_{init}, as observed in 10% or 20% of failures in Fig. 1a and in 20% or 30% in Fig. 2a, as well as in the targeted-based surfaces. This result should not be misleading because it totally depends on the set of metrics that are being considered for the study. For instance, while some metrics might decrease as the percentage of failures increases, others might alternate increments and decrements because they depend on the number and size of largest connected components (i.e., average shortest-path length, diameter, algebraic connectivity, etc.). Therefore, the suitability of the robustness surface remains intact, because the variability of the robustness can be assessed in any case.

Finally, to compare the robustness surfaces of both networks, and considering the different failure scenarios, we average the values of each ω'_p of Ω. Thus, for each network and failure scenario, we obtain $|P|$ $\bar{R}^*_p$-values. Fig. 3 depicts a summary of the results. Fig. 3a shows the curves of $\bar{R}^*_p$ of both networks from 1% to 70% of failures. To complement the results in Fig. 3a, the variance is presented in Fig. 3b. For instance, it can be observed that both random failure scenarios show similar behaviors, although for *europg* the top of the curve is around 24% of failures. Therefore, our approach allows us to compare different networks, regardless of the failure scenarios. This comparison could be done numerically, for instance, by comparing the areas below the curves.

Discussion

In this work we present the R^*-value and the concept of *robustness surface* (Ω). The rationale of our proposal is to make use of Principal Component Analysis (PCA).

The R^*-value solves two open issues in the robustness of complex networks field. Our proposal extracts the most significant information from a set of robustness metrics. R^* is the first generic metric able to characterize the robustness of complex networks with a single value, while taking into account several robustness metrics.

The robustness surface Ω provides a framework to visually assess the network robustness variability. Moreover, it allows for the comparison of the robustness between different networks under distinct failure scenarios. To the best of our knowledge, it is the first method of its kind to allow the visual evaluation of the network robustness for a specific failure scenario, while at the same time considering several robustness metrics.

Robustness surfaces are designed as a visual monitoring tool. First, our approach is applicable to real-time monitoring of a network through a single value, when it is otherwise implemented according to multiplicity of correlated metrics with possible inherent redundancy. Second, Ω can be a pivotal part of a network robustness refinement process:

- Step 1: If the robustness surface presents abrupt slopes, then there are network elements (nodes or links) which are weaker than the rest, for a given failure scenario. These elements could be identified by means of traditional robustness metrics such as the betweenness centrality.
- Step 2: Enhance or protect the weak elements, for instance, by adding new links or applying immunization techniques.
- Step 3: Re-evaluate the robustness of a network and, instead of comparing a large number of robustness metrics, detect through visual inspection if the network robustness has been improved.

We believe that the contributions presented in this work will lay a firm foundation for future research on the robustness of complex networks.

To conclude, the R^*-value shows that there is no single and universal robustness metric for a network. Instead, the robustness varies according to the failure scenario and the metrics that are used to quantify the performance of the network.

For future work, we plan to study the stability of the robustness surfaces with respect to network size scaling.

Methods

Principal Component Analysis (PCA). PCA is a powerful tool to identify the most significant information in a data table representing observations described by several dependent variables, which can be inherently correlated. The goals of the PCA are to: (a) extract the main information of a data set and express it by means of new orthogonal variables called principal components; and (b) compress the size of the data set while preserving the most important information [23].

Let A be a data set of m observations of a vector-valued variable, i.e., $A \in R^{m \times n}$. We define C as the covariance matrix of A, which is denoted by:

$$C^{n \times n} = (c_{i,j}, c_{i,j} = cov(col_{A_i}, col_{A_j})) \tag{5}$$

where $i, j \in \{1..n\}$, and $cov(col_{A_i}, col_{A_j})$ is the covariance function evaluating column i and column j.

PCA works with the spectrum of C. Let $v_i \in R^{n \times 1}\{i \in 1..n\}$ and $\lambda_i \in R$ be the eigenvectors and corresponding eigenvalues of the covariance matrix C, respectively. The matrix V with all v_i as columns represents the principal components, and provides an orthogonal transformation to the PC space. Furthermore, we denote D as a matrix with the eigenvalues in its diagonal.

Let $\tilde{V}$ be $n \times l$ matrix, which only contains the top l of the most important principal components (see *Methods: Most relevant principal components of A* for further details). Therefore, we can obtain the transformed data $\omega = A\tilde{V}$.

In our problem, each failure has a covariance matrix C_p, where p is the percentage of failure. We perform the PCA on $\bar{C} = \int C_p \delta p$, in order to obtain the PC independent of p.

Most relevant principal components of A. In order to choose the l most relevant principal components, matrices V (eigenvectors) and D (eigenvalues) must be column-sorted in decreasing order, according to the eigenvalues in the diagonal of D. The importance of each eigenvector is characterized

by its energy quantum g. The eigenvalues represent the distribution of the energy of A among each of the eigenvectors. The energy quantum for the j_{th} eigenvector is the sum of the energy quantum across all eigenvalues from 1 to j:

$$g[j] = \sum_{k=i}^{j} D[k][k] \quad j = 1..n \quad . \tag{6}$$

Let $\tilde{V}$ be an $n \times l$, where $l \leq n$ matrix that contains the most relevant eigenvectors. Then, the objective is to choose an l value as low as possible while preserving a reasonable high value of g on a percentage basis. For instance, we have chosen l so that g is above a certain threshold α:

$$min\{l \in [1..n] : \frac{g[l]}{g[n]} \geq \alpha\} \tag{7}$$

In this work we have considered $\alpha = 0.9$, from which we have obtained $l = 1$.

Simulation details. The computation of each metric has been done with PHISON [24]. The simulations were performed on a Linux system with a 16-core 64-bit Intel Xeon processor of 2Ghz and 64 GB of RAM. The presented results are the average of 500 and 100 differently seeded simulation runs for random and targeted failures, respectively. The figures have been plotted by means of the *pcolor* function of MATLAB. In addition, the PCA has also been done with MATLAB.

Acknowledgments

This work is partially supported by the Spanish Ministry of Science and Innovation project TEC 2012-32336, and by the Generalitat de Catalunya research support program SGR-1202. This work is also partially supported by the Secretariat for Universities and Research (SUR) and the Ministry of Economy and Knowledge through AGAUR FI-DGR 2012 and BE-DGR 2012 grants.

References

[1] Albert, R., Jeong, H. & Barabasi, A. Error and attack tolerance of complex networks. *Nature* **406**, 378–382 (2000).

[2] Manzano, M., Calle, E., Torres-Padrosa, V., Segovia, J. & Harle, D. Endurance: A new robustness measure for complex networks under multiple failure scenarios. *Computer Netw.* **57**, 3641–3653 (2013).

[3] Sydney, A., Scoglio, C., Youssef, M. & Schumm, P. Characterising the robustness of complex networks. *Int. J. Internet Technol. Secur. Syst.* **2**, 291–320 (2010).

[4] Manzano, M., Calle, E. & Harle, D. Quantitative and qualitative network robustness analysis under different multiple failure scenarios. In *Proceedings of the 3rd International Workshop on Reliable Networks Design and Modeling (RNDM)*, 1–7 (2011).

[5] Latora, V. & Marchiori, M. Efficient behavior of small-world networks. *Phys. Rev. Lett.* **87**, 198701 (2001).

[6] Watts, D. J. & Strogatz, S. H. Collective dynamics of 'small-world' networks. *Nature* **393**, 440–442 (1998).

[7] Shannon, C. & Moore, D. The Spread of the Witty Worm. *IEEE Secur. Priv.* **2**, 46–50 (2004).

[8] Albert, R., Jeong, H. & Barabási, A. Internet: Diameter of the world-wide web. *Nature* **401**, 130–131 (1999).

[9] Bollobás, B. Mathematical results on scale-free random graphs. In *Handbook of Graphs and Networks*, 1–34 (Wiley-VCH, 2003).

[10] Dekker, A. H. & Colbert, B. D. Network robustness and graph topology. In *Proceedings of the 27th Australasian conference on Computer science - Volume 26, ACSC, Australian Computer Society*, 359–368 (2004).

[11] Dong, J. & Horvath, S. Understanding network concepts in modules. *BMC Syst. Biol.* **1**, 1–24 (2007).

[12] Neumayer, S. & Modiano, E. Network reliability with geographically correlated failures. In *Proceedings of the 29th conference on Information Communications (INFOCOM)*, 1658–1666 (2010).

[13] Mahadevan, P. *et al.* The internet AS-level topology: three data sources and one definitive metric. *SIGCOMM Comput. Commun. Rev.* **36**, 17–26 (2006).

[14] Freeman, L. C. A set of measures of centrality based upon betweenness. *Sociometry* **40**, 35–41 (1977).

[15] Dekker, A. H. & Colbert, B. D. The symmetry ratio of a network. In *Proceedings of the 2005 Australasian symposium on Theory of computing - Volume 41, CATS, Australian Computer Society*, 13–20 (2005).

[16] Jamakovic, A. & Mieghem, P. V. On the Robustness of Complex Networks by Using the Algebraic Connectivity. In *Proceedings of Networking*, vol. 4982, 183–194 (2008).

[17] Van Mieghem, P., Omic, J. & Kooij, R. Virus Spread in Networks. *IEEE/ACM Trans. Netw.* **17**, 1–14 (2009).

[18] Rohrer, J. P. & Sterbenz, J. P. G. Predicting Topology Survivability using Path Diversity. In *Proceedings of the 3rd International Workshop on Reliable Networks Design and Modeling (RNDM)*, 1–7 (2011).

[19] Trajanovski, S., Martín-Hernández, J., Winterbach, W. & Van Mieghem, P. Robustness envelopes of networks. *J. Complex Netw.* (2013).

[20] Van Mieghem, P. *et al.* A framework for computing topological network robustness. *Technical Report 20101218, Networks Architectures and Services, Delft University of Technology* (2010).

[21] Roanes-Lozano, E. *et al.* Evolution of railway network flexibility: The Spanish broad gauge case. *Math. Comput. Simul.* **79**, 2317–2332 (2009).

[22] Hutcheon, N. & Bialek, J. W. Updated and validated power flow model of the main continental european transmission network. In *Proceedings of the IEEE PowerTech 2013* (2013).

[23] Abdi, H. & Williams, L. J. Principal component analysis. *Computation. Stat.* **2**, 433–459 (2010).

[24] Manzano, M., Segovia, J., Calle, E. & Marzo, J. L. PHISON: Playground for High-level Simulations On Networks. In *Proceedings of the 2012 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)* (2012).

Table 1: Definition of the variables.

Variable	Meaning
n	number of robustness metrics
R	R-value [20]
s	vector of weights (size $n \times 1$)
t	vector of metrics (size $n \times 1$)
m	failure configurations, i.e., different realizations of the failure process
R^*	R-value computed via Principal Components (PC)
t^0	vector of metrics without failures (size $n \times 1$)
R^*_{init}	initial R^*-value (without failures)
v	eigenvector PC (size $n \times 1$)
$\hat{v}$	normalized eigenvector PC (size $n \times 1$)
P	set of percentage of failures
p	percentage of failures ($p \in P$)
t^p	vector of metrics when p% of elements fail
R^*_p	R-value when p% of elements fail
A_p	$m \times n$ matrix, i.e., m values for each of the n metrics when p% of elements fail
ω_p	vector of R^*_p values (size $m \times 1$)
ω'_p	vector ω_p sorted in decreasing order
C_p	covariance matrix of A_p (size $n \times n$)
$\bar{C}$	average of the $\|P\|$ covariance matrices (size $n \times n$)
V	matrix containing n eigenvectors v
D	diagonal matrix with eigenvalues (size $n \times n$)
l	number of most relevant eigenvector
Ω	robustness surface, i.e., $\|P\|$ vectors ω'_p

Table 2: Main network characteristics. The table displays, from left to right, topology name, number of nodes (N), number of links (L), average node degree ± *standard deviation* (StDev) ($\langle k \rangle$), maximum degree ($k_{\max}$), average shortest-path length ± StDev ($\langle l \rangle$) and assortativity (r).

topology	N	L	$\langle k \rangle$ ± StDev	$k_{\max}$	$\langle l \rangle$ ± StDev	r
sprailway	169	190	2.24 ±1.09	8	10.49 ±4.64	-0.269
europg	1,494	2,154	2.88 ±1.75	13	18.88 ±8.73	-0.119

Epidemic and Cascading Survivability of Complex Networks

Marc Manzano, Eusebi Calle, Jordi Ripoll, Anna Manolova Fagertun,
Victor Torres-Padrosa, Sakshi Pahwa, Caterina Scoglio

Abstract

Our society nowadays is governed by complex networks, examples being the power grids, telecommunication networks, biological networks, and social networks. It has become of paramount importance to understand and characterize the dynamic events (e.g. failures) that might happen in these complex networks. For this reason, in this paper, we propose two measures to evaluate the vulnerability of complex networks in two different dynamic multiple failure scenarios: epidemic-like and cascading failures. Firstly, we present *epidemic survivability* (ES), a new network measure that describes the vulnerability of each node of a network under a specific epidemic intensity. Secondly, we propose *cascading survivability* (CS), which characterizes how potentially injurious a node is according to a cascading failure scenario. Then, we show that by using the distribution of values obtained from ES and CS it is possible to describe the vulnerability of a given network. We consider a set of 17 different complex networks to illustrate the suitability of our proposals. Lastly, results reveal that distinct types of complex networks might react differently under the same multiple failure scenario.

Index Terms

Network Characterization, Epidemics, Cascading Failures, Multiple Failures, Complex Networks

I. Introduction

Telecommunication networks, power grids, water distribution networks, transport networks or fuel distribution networks are critical infrastructures that play a vital role in our modern society. Such crucial networks do not display regular organizations, ergo they have also been addressed as *complex networks*. The study of complex networks not only comprises critical infrastructures, but also any other kind of network with non-trivial features. Social networks, biological networks, online social networks and mobile social networks [1] are solid examples of complex networks.

Our society of nowadays is governed by complex networks. For instance, people have become more and more dependent on communication networks, either for business or leisure purposes. In addition, this dependency is expected to grow, considering the myriad of new emerging technologies and services such as smart-cities, cloud

Marc Manzano, Eusebi Calle, Jordi Ripoll and Victor Torres-Padrosa are with University of Girona, Spain. Anna Manolova Fagertun is with Technical University of Denmark, Denmark. Sakshi Pahwa and Caterina Scoglio is with Kansas State University, USA. Corresponding author: Marc Manzano (email: mmanzano@eia.udg.edu - marcmanzano@ksu.edu).

computing, e-Health, the Internet of the Things, MANETs, etc. Consequently, the period of time for which a user can operate terminals without network connectivity is becoming very short; and if a large-scale failure occurred, it would impact a significant percentage of the world's population. Another example is the online social networks such as Twitter or Facebook. In August 2013 a single tweet of a billionaire investor made Apple shares rise over $500 [2], showing how a single message can spread and reach millions of users within hours. These two examples depict how important it is to understand the events that might occur on complex networks. From now on, in this work we are going to use the term *failure* to refer to any event that causes disruption in the normal functioning of a complex network.

Many different protection and restoration techniques for single failures have been extensively analyzed in recent decades (e.g. see [3]). Furthermore, multiple failures such as natural disasters or physical attacks have also been studied [4]. According to the taxonomy introduced in [5], there are two types of multiple failures. While *static* multiple failures are essentially one-off failures that affect one or more elements (nodes or links) simultaneously at any given point, *dynamic* failures have a temporal dimension. In this paper we consider *dynamic* multiple failures, which we implement through *epidemic* and *cascading* failures. On one hand, an epidemic-like failure propagation occurs when, at a given time, a node or a group of them start spreading an infection. In this case the failure (e.g. infection) propagates through physical neighbors. On the other hand, cascading failures occur when a node (or a group of them) fails, and as a consequence, other parts in the network fail as well due to an overloading of the capacity. Cascading failures do not necessarily propagate through physical contact, i.e. one node failure can cause a failure to a non-adjacent node due to the network load balancing.

In contrast with single failures, in the case of multiple failures it is nonviable to define proper reactive strategies. Thus, since the reasonable approach to address such large-scale failures involves the designing phase of a network, it has become of paramount importance to define new metrics able to evaluate the vulnerability of networks in the case of multiple failure scenarios. Appropriate metrics can help network engineers and operators to detect the most critical parts of a network. Although a new generic metric suitable to accurately evaluate the robustness in static multiple failure scenarios has been recently presented in [5], to the best of our knowledge there are no metrics able to evaluate the robustness under dynamic multiple failure scenarios.

In our previous work [6] we presented a metric called epidemic survivability. In this paper we go one step further and we extend the work by considering broader type of failures: dynamic multiple failures. In addition, we extend the number of networks considered for testing of the failure scenarios to 17, as compared to 6 in the previous work. Consequently, here we consider 2 telecommunication networks, 2 Internet Autonomous Systems (AS) networks, 5 synthetic generated networks, 1 biological network, 3 social networks and 4 power grid networks. Our aim is to take into account a wide range of different types of complex networks, and evaluate them under dynamic multiple failure scenarios. Within this context, the main contributions of this paper are:

1) a new network measure called *epidemic survivability* (ES). This feature describes the vulnerability of each node of a network under a specific epidemic scenario.
2) a new network measure called *cascading survivability* (CS), which characterizes how potentially injurious a

node is according to a specific cascading failure scenario.

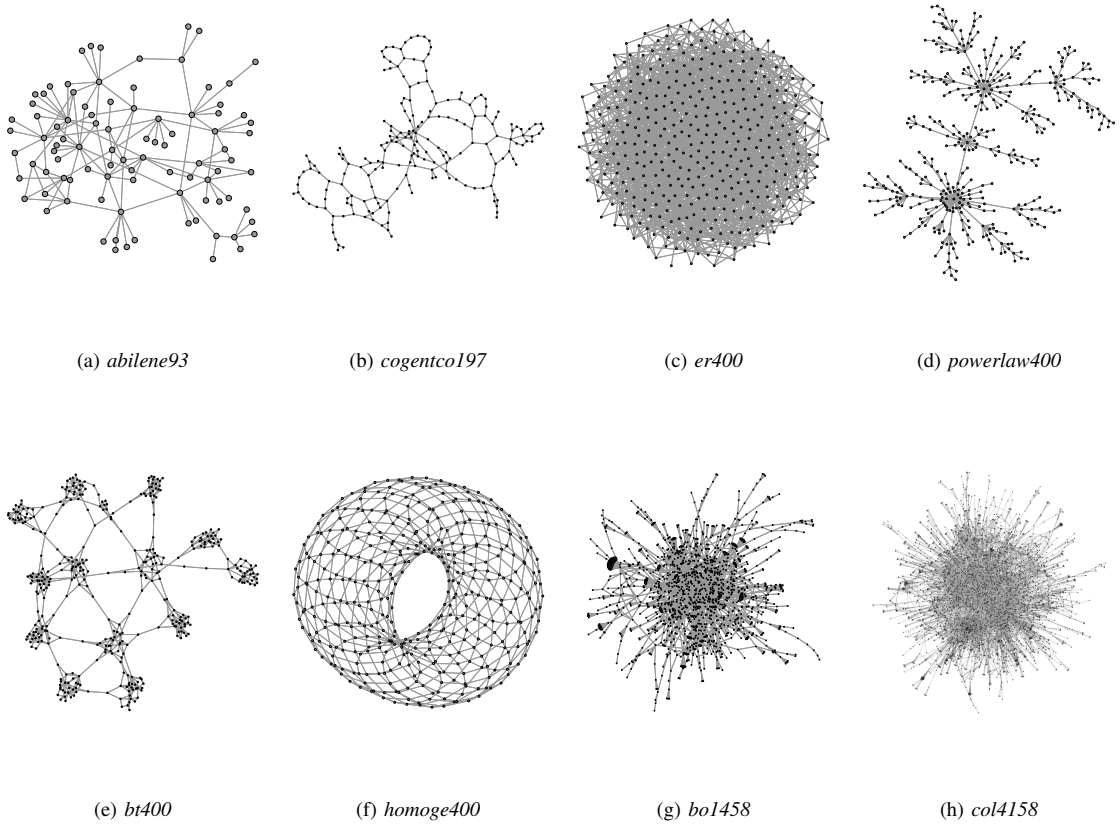
We believe that our proposals can be used by the network research community to evaluate the criticality of nodes of a network under failure propagation scenarios. In addition, our metrics can be used to amplify general recovery metrics such as [7].

The remainder of this work is organized as follows: Section II presents the set of network topologies considered in this paper. In Section III we (a) introduce the state of the art related with epidemic failures; (b) review the most well-known epidemic models; (c) present our new network measure called *epidemic survivability*; and (d) show a practical example of how could our proposal be used. Then, Section IV (a) provides a background with respect to cascading failures; (b) presents several remarkable cascading failure models; (c) defines our new metric called *cascading survivability*; and (d) illustrates how to use the metric. Finally, Section V concludes this work reviewing its main contributions and findings.

II. Network Topologies

In this section we present the set of seventeen network topologies considered in our work. These networks have been chosen in order to represent a wide variety of complex network topology types. Generating representative synthetic topologies is a difficult task (and it is not the objective of this paper). Thus, we have conducted an extensive investigation and we have obtained seventeen networks from several sources, which are described next (the name of each network includes the number of nodes):

1) *abilene93* (Fig. 1a): a small network that has been chosen because of its underlying AS topology structure.
2) *cogentco197* (Fig. 1b): a real telecommunications network that has been taken from the repository provided in [8].
3) *er400* (Fig. 1c): a random network that has been generated using the Erdős-Rényi model [9].
4) *powerlaw400* (Fig. 1d): a power-law network that has been generated using the Barabási-Albert (BA, preferential attachment mechanism) model [10].
5) *homoge400* (Fig. 1f): a homogeneous network (a network where all the nodes have equal node degree) that has been generated, being a toroidally-periodic rectangular lattice of size 20×20. Although this network is not a complex network, it has been considered for comparison purposes.
6) *bt400* (Fig. 1e): this topology has been obtained by manipulating a previously generated topology using BRITE.
7) *bo1458* (Fig. 1g): a protein interaction network for yeast [11].
8) *col4158* (Fig. 1h): a collaboration network of Arxiv's *General Relativity* category [12].
9) *col8638* (Fig. 2a): a collaboration network of Arxiv's *High Energy Physics Theory* category [12].
10) *cost37* (Fig. 2b): a Pan-european communications reference network.
11) *europg1494* (Fig. 2c): an approximated model of the european power grid network [13].
12) *fb4039* (Fig. 2d): this network represents *circles* or *friends list* of the popular social network Facebook [14].
13) *wspg4941* (Fig. 2e): a topology of the Western States Power Grid of the United States [15].



(a) *abilene93* (b) *cogentco197* (c) *er400* (d) *powerlaw400*

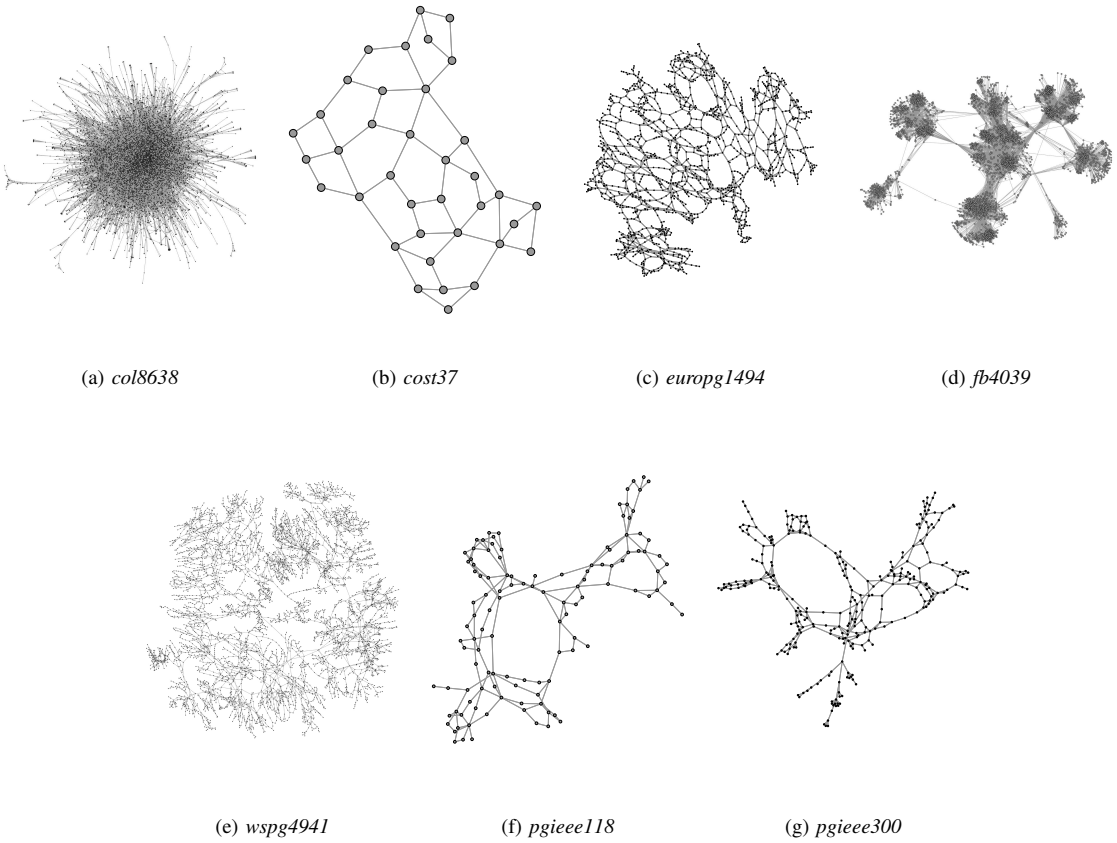
(e) *bt400* (f) *homoge400* (g) *bo1458* (h) *col4158*

Fig. 1. Layout of 8 out of the 17 topologies considered in this work.

14) *pgieee118* and *pgieee300* (Fig. 2f and Fig. 2g): these two topologies are reference IEEE power grid networks [16].
15) *AS25357*: an AS network from 2012 [17].
16) *AS26475*: this network is the largest CAIDA AS connected graph from the network set available in November 2007 [12].

The *col4158*, *col8638*, *fb4039* and *AS26475* networks have been obtained from the SNAP dataset [18]. The layouts of 15 of the 17 topologies can be observed in Figs. 1 and 2. All of the networks are connected and considered as symmetric graphs. It is worth noting that some of the networks were not connected, and a post-processing has been done in order to obtain the largest connected component. Table I shows the networks that have been post-processed because they were disconnected. Furthermore, Table II and Table III present several characteristics of this set of networks, some of which are presented with their *standard deviation*. As it can be observed, we have considered a heterogeneous set of networks with respect to the number of nodes, ranging from 37 to 26475.

The *fb4039* network shows the highest average nodal degree ($\langle k \rangle = 43.69$), what means that every person has an average of about 44 friends in this social network. The two AS networks (*AS25357* and *AS26475*) present the



(a) *col8638* (b) *cost37* (c) *europg1494* (d) *fb4039*

(e) *wspg4941* (f) *pgieee118* (g) *pgieee300*

Fig. 2. Layout of 7 out of the 17 topologies considered in this work.

TABLE I

NETWORKS THAT WERE DISCONNECTED AND FOR WHICH A POST-PROCESSING HAS BEEN DONE TO OBTAIN THE LARGEST CONNECTED COMPONENT.

Topology	List of $\|N\|\times$ number of components
bo1458	1458×1; 7×4; 6×3; 5×5; 4×10; 3×25; 2×101; 1×24
col4158	4158×1; 14×1; 12×1; 10×1; 9×2; 8×6; 7×8; 6×12; 5×17; 4×30; 3×98; 2×177; 1×1
col8638	8638×1; 21×1; 11×1; 9×2; 8×6; 7×11; 6×8; 5×21; 4×45; 3×67; 2×264; 1×2
europg1494	1494×1; 1×19
AS25357	25357×1; 2×5

TABLE II

MAIN NETWORK FEATURES. THE TABLE DISPLAYS, FROM LEFT TO RIGHT: TOPOLOGY NAME, NUMBER OF NODES, AVERAGE NODAL DEGREE $\pm$ *standard deviation* (STDEV), MEAN DEGREE OF FIRST NEIGHBORS $\pm$ STDEV, LARGEST EIGENVALUE OF THE ADJACENCY MATRIX, MAXIMUM DEGREE $k_{\max}$ AND THE SECOND SMALLEST EIGENVALUE OF THE LAPLACIAN MATRIX (THE SO-CALLED *algebraic connectivity*).

Topology	N	$\langle k \rangle \pm$ StDev	$\langle d \rangle \pm$ StDev	λ_1	$k_{\max}$	μ_{N-1}
abilene93	93	2.88 $\pm$2.71	6.76 $\pm$2.76	5.016	12	0.07607
cogentco197	197	2.46 $\pm$1.05	2.91 $\pm$0.92	3.778	9	0.00858
er400	400	7.81 $\pm$2.80	8.89 $\pm$1.01	8.848	15	0.90416
powerlaw400	400	2.00 $\pm$3.25	9.47 $\pm$11.81	7.013	47	0.00463
homoge400	400	4.00 $\pm$0.00	4.00 $\pm$0.00	4.000	4	0.09788
bt400	400	3.74 $\pm$2.17	5.44 $\pm$1.61	5.195	11	0.01013
bo1458	1458	2.67 $\pm$3.45	9.65 $\pm$10.74	7.535	56	0.02126
col4158	4158	6.45 $\pm$8.62	11.60 $\pm$9.02	45.616	81	0.03530
col8638	8638	5.74 $\pm$6.45	11.25 $\pm$6.65	31.034	65	0.02441
cost37	37	3.08 $\pm$0.85	3.31 $\pm$0.45	3.399	5	0.15857
europg1494	1494	2.88 $\pm$1.75	4.17 $\pm$1.58	5.027	13	0.00170
fb4039	4039	43.69 $\pm$52.41	105.55 $\pm$91.30	162.373	1045	0.01812
wspg4941	4941	2.66 $\pm$1.79	3.96 $\pm$1.93	7.483	19	0.00076
pgieee118	118	3.03 $\pm$1.56	3.95 $\pm$1.13	4.105	9	0.02714
pgieee300	300	2.72 $\pm$1.54	3.86 $\pm$1.71	4.126	11	0.00938
AS25357	25357	5.91 $\pm$48.03	659.73 $\pm$827.98	103.361	3781	0.10768
AS26475	26475	4.03 $\pm$33.37	471.27 $\pm$644.72	69.642	2628	0.02043

highest mean degree of first neighbors ($\langle d \rangle$) and maximum degree ($k_{\max}$), i.e. in *AS25357* there is an AS that is connected to other ($k_{\max}$) 3781 ASes, and some of them have a high node degree as well. A high $k_{\max}$ is an indicator of vulnerability, depicting that removal of such a node could seriously damage the network. Networks with high values of the largest eigenvalue of the adjacency matrix (or spectral radius, λ_1) and algebraic connectivity (μ_{N-1}) are more robust. In this case, the *fb4039* network shows the highest spectral radius and the *er400* presents the highest algebraic connectivity. For this reason, these two networks are supposed to be most robust than the rest of them in the case of failures.

Regarding the average shortest-path length ($\langle l \rangle$) it is shown that two power grid networks (*europg1494* and *wspg4941*) have the higher values and consequently are more vulnerable. This is due to the fact that, traditionally, power grid networks have a tree-like structure. Furthermore, the average node betweenness centrality ($\langle b \rangle$) of *cost37*, *cogentco197* and *abilene93* shows that these three topologies have an excess of centrality measures for some nodes, indicating the vulnerability of networks under targeted failures. The absence of 3-cycles in the clustering coefficient ($\langle C \rangle$) measurements reveal that the *homoge400* and *cost37* lack two-hop paths to re-route the traffic in case of failure of one of its neighbors. Finally, networks with negative values of assortativity (r) have an excess of radial links, i.e., links connecting nodes of dissimilar degrees. Such a property is typical of technological networks [19].

TABLE III

NETWORK FEATURES. THE TABLE DISPLAYS, FROM LEFT TO RIGHT: TOPOLOGY NAME, AVERAGE SHORTEST PATH LENGTH $\pm$ STDEV, NORMALIZED AVERAGE BETWEENNESS CENTRALITY $\pm$ STDEV, AVERAGE CLUSTERING COEFFICIENT $\pm$ STDEV, AND ASSORTATIVITY COEFFICIENT $|r| \leq 1$.

Topology	$\langle l \rangle \pm$ StDev	$\langle b \rangle \pm$ StDev	$\langle C \rangle \pm$ StDev	r
abilene93	3.92 $\pm$1.32	0.0529 $\pm$0.0551	0.51 $\pm$0.48	-0.5130
cogentco197	10.52 $\pm$5.09	0.0585 $\pm$0.0665	0.12 $\pm$0.32	$+0.01956$
er400	3.13 $\pm$0.73	0.0103 $\pm$0.0037	0.02 $\pm$0.07	-0.07229
powerlaw400	6.01 $\pm$2.16	0.0175 $\pm$0.0594	0.64 $\pm$0.47	-0.16512
homoge400	10.03 $\pm$4.10	0.0276 $\pm$0.0000	0.00 $\pm$0.00	$+1.0000$
bt400	10.12 $\pm$4.21	0.0202 $\pm$0.0357	0.16 $\pm$0.27	-0.29646
bo1458	6.81 $\pm$2.04	0.0039 $\pm$0.0110	0.56 $\pm$0.47	-0.20954
col4158	6.04 $\pm$1.57	0.0012 $\pm$0.0034	0.71 $\pm$0.35	$+0.63919$
col8638	5.94 $\pm$1.50	0.0005 $\pm$0.0015	0.65 $\pm$0.37	$+0.23892$
cost37	4.05 $\pm$1.90	0.0782 $\pm$0.0756	0.00 $\pm$0.00	-0.01510
europg1494	18.88 $\pm$8.73	0.0119 $\pm$0.0304	0.27 $\pm$0.40	-0.11965
fb4039	3.69 $\pm$1.19	0.0006 $\pm$0.0116	0.62 $\pm$0.20	$+0.06358$
wspg4941	18.98 $\pm$6.50	0.0036 $\pm$0.0160	0.32 $\pm$0.44	$+0.00346$
pgieee118	6.30 $\pm$2.81	0.0457 $\pm$0.0723	0.22 $\pm$0.36	-0.15257
pgieee300	9.93 $\pm$4.06	0.0299 $\pm$0.0546	0.31 $\pm$0.42	-0.22063
AS25357	3.39 $\pm$0.70	0.0001 $\pm$0.0020	0.73 $\pm$0.36	-0.18540
AS26475	3.87 $\pm$0.90	0.0001 $\pm$0.0020	0.58 $\pm$0.46	-0.19465

This initial network analysis of the considered set of topologies reveals that none of the networks can be considered as the most robust for all of the metrics. Besides, the vulnerability of the networks is going to differ depending on the considered type of multiple failures. As a consequence, it is necessary to define new metrics able to characterize how robust a network is in a specific scenario. The following two sections present two new measures to evaluate network vulnerability in the case of epidemic-like and cascading failures.

III. EPIDEMIC-LIKE FAILURES

Throughout the history of mankind there have been many diseases that have spread quickly, becoming an epidemic or even a pandemic. As a result, many epidemic outbreaks have ravaged human civilizations from the Middle Ages until today. For instance, the devastating Influenza epidemic of 1918 (the third greatest plague in history) claimed 21 million lives and affected over half the world's population [20].

Epidemic models are used to model the spreading of events (e.g. failures) in several types of complex networks. These models have been used in a wide variety of research fields. For instance, in [21] the authors used characteristics of epidemic spreading to model the fire propagation on a forest. In [22], the authors used epidemic models to show that emotional states spread like infectious diseases across social networks. In [23] it was shown that there are certain network structures that facilitate the propagation of new ideas, behaviors or technologies. In the last years,

online social networks (OSNs) have also been the focus of study. For instance, in [24] the authors studied how to control virus propagation in OSNs. Finally, although no commercial references (or reports) have been found with respect to the propagation of failures in telecommunication networks, several works have focused on analyzing the consequences of epidemic attacks on the services provided by such networks [25], [26], [27]. Additionally, a framework to eradicate epidemic failure has been recently proposed in [28]. Nonetheless, to the best of our knowledge, no methods to detect the most vulnerable nodes of a complex network in the case of epidemic failures have been proposed. Therefore, a first step would be to define network measures to characterize all nodes under such failure scenarios.

A. Epidemic Models

Epidemic dynamics in complex networks have undergone extensive research [29], [30] [31], [32], [33]. As a consequence, many epidemic models have been proposed and several families are described in the literature (see Chapter 8 in [34], Chapter 17 in [35] and Chapter 14 in [36]). The first family, called *Susceptible-Infected* (SI) considers individuals as being either susceptible (S) or infected (I). This family assumes that the infected individuals will remain infected forever, and so can be used for worst case propagation ($S \rightarrow I$). Another family is the *Susceptible-Infected-Susceptible* (SIS) group, which considers that a susceptible individual can become infected on contact with another infected individual, then recovers with some probability of becoming susceptible again. Therefore, individuals will change their state from susceptible to infected, and vice versa, several times ($S \leftrightarrows I$). The *Susceptible-Exposed-Infected-Susceptible* (SEIS) model is based on the SIS model, and takes into consideration the exposed or latent period of the disease ($S \rightarrow E \rightarrow I \rightarrow S$). The third broad family is *Susceptible-Infected-Removed* (SIR), which extends the SI model to take into account a removed state. In the SIR model, an individual can be infected just once because when the infected individual recovers, becomes either immune or dead, and will no longer pass the infection onto others ($S \rightarrow I \rightarrow R$). Finally, there are two families that extend the SIR family: *Susceptible-Infected-Detected-Removed* (SIDR) and *Susceptible-Infected-Removed-Susceptible* (SIRS). The first one adds a Detected (D) state, and is used to study virus throttling, which is an automatic mechanism for restraining or slowing down the spread of diseases ($S \rightarrow I \rightarrow D \rightarrow R$). The second one considers that after an individual becomes removed, it remains in that state for a specific period of time and then goes back to the susceptible state ($S \rightarrow I \rightarrow R \rightarrow S$).

Regarding communication networks, an extension of the SIS model, which is called Susceptible-Infected-Disabled-Susceptible (SIDS), was proposed in [25] in order to overcome the limitations of the SIS model with respect to optical transport networks. The SIDS model (*Susceptible*$\leftrightarrows$*Infected*$\rightarrow$*Disabled*$\rightarrow$*Susceptible*) is proposed as one of the first models to consider real telecommunication networks features and it relates each state to a functionality of the network devices. In addition, other epidemic models have also been proposed for wireless telecommunication networks [37].

In this paper we propose a new network measure taking into account the SIS model, which is characterized by two probabilities: (a) β, the probability of being infected by an already infected node; and (b) δ, the probability of

an infected node to recover and become susceptible again. However, our proposal can be also applied to any other epidemic model and we plan to do so in the future.

Furthermore, according to [33] and from the following equation:

$$s = \frac{\beta}{\delta}\lambda_1 \tag{1}$$

where s is the *epidemic intensity* and λ_1 is the network's largest eigenvalue of the adjacency matrix, which has been typically used to predict network robustness, when $s > 1$ an epidemic survives and the spread of the infection might never die. Thus, in order to obtain comparable results between networks with respect to our proposal (*epidemic survivability*), s must be a parameter of our new measure.

In this work we have fixed $s = 3$ for all networks, in order to obtain comparable results, and we have obtained a specific β value for each network from the equation $\beta = \frac{s\delta}{\lambda}$.

B. Epidemic Survivability

Here we present our new network measure called *epidemic survivability* (ES). We define our proposal as the probability for each node of a given network to be eventually infected (i.e., in a large enough amount of time steps), given a specific *epidemic intensity* (s). This probability of each node asymptotically reaches a stationary state, according to simulations and theoretical models. *Epidemic survivability* can be described as the proportion of time for which each node of a given network has been infected for a given s, in a large enough period of time, as shown in Eq. 2:

$$ES_i(s) = \frac{\text{time for which node } i \text{ has been infected}}{\text{total time}} \qquad i = 1, \ldots, N \tag{2}$$

where N is the number of nodes of the network. As a result, ES has a value between 0 and 1 for each node, where higher the value, more vulnerable is the node under the specified epidemic scenario. Formally, from the SIS model, *epidemic survivability* can be computed with the following equation:

$$ES_i^* = \frac{1}{1 + (\frac{\beta}{\delta}\sum_{j\sim i} ES_j^*)^{-1}} \qquad i = 1, \ldots, N \tag{3}$$

where $*$ means *at the stationary state* and $j \sim i$ is the set of *neighbors* of node i. Here, it is assumed that δ and s are given as parameters and β is obtained from the equation $\beta = \frac{s\delta}{\lambda_1}$. Thus, it can be observed that Eq. 3 is a recursive formula and must be initialized with a value. We define this initialization of the probabilities in Eq. 4:

$$ES_{i,\text{approx}}^* = (1 - \frac{1}{s}) \qquad i = 1, \ldots, N \tag{4}$$

which corresponds to the solution of Eq. 3 for the case of a homogeneous/regular network. Moreover, a procedure for computing *epidemic survivability* is provided in Algorithm 1. As it can be observed, the method requires five parameters: the network $\mathcal{G}$ and four constants (s, δ, k and tol). The first two steps (lines 3 and 4) compute the largest eigenvalue of the given network and thus obtain the β value of the epidemic model. Then, all probabilities

are initialized as stated in Eq. 4 (lines 5 to 7). Therefore, in the main loop of line 8 the new probability of each node is computed as defined in Eq. 3 (lines 9 to 11). After that, the absolute error is checked (lines 12 to 14) and if it results lower than the given tolerance (tol) then the algorithm ends, and returns the array containing the *epidemic survivability* of each node of the network. If the absolute error is still higher than tol another iteration is performed.

Algorithm 1 Compute *epidemic survivability*.

Require: $s \geq 1, d > 0, k > 0, tol > 0, connected\ \mathcal{G}$

1: **Input:** a graph $\mathcal{G}$ and the constants s (epidemic intensity), δ (repairing rate), k (maximum number of iterations) and tol (tolerance).
2: **Output:** an array containing the *epidemic survivability* of each node.
3: $\lambda \leftarrow$ spectralRadius($\mathcal{G}$) {largest eigenvalue}
4: $\beta \leftarrow \frac{s*\delta}{\lambda}$
5: **for all** $v \in vertexSet(\mathcal{G})$ **do**
6: $\quad P_{ES}[v] = (1 - \frac{1}{s})$
7: **end for**
8: **for** $c = 1 \rightarrow k$ **do**
9: $\quad$ **for all** $v \in vertexSet(\mathcal{G})$ **do**
10: $\quad\quad P_{aux}[v] = \frac{1}{1+(\frac{\beta}{\delta} \sum_{j \sim v} P_{ES}[j])^{-1}}$
11: $\quad$ **end for**
12: $\quad$ **if** $(\|P_{aux} - P_{ES}\|) < tol$ **then**
13: $\quad\quad$ break
14: $\quad$ **end if**
15: $\quad P_{ES} \leftarrow P_{aux}$
16: **end for**
17: **return** P_{ES}

C. The distribution

When computing the *epidemic survivability* for the nodes of a network, according to a specified set of parameters, it is interesting to analyze the distribution of ES values. If these values are sorted, for example, in descending order, it facilitates the comparison between network topologies when considering the same failure propagation scenario for all of them. This approach is illustrated in Fig. 3 which displays the *epidemic survivability* distribution, the ES of each node, for the 17 networks in a specific epidemic scenario. As can be observed, the two AS networks (*AS25357* and *AS26475*) together with the two collaboration networks (*col4158* and *col8638*) show the lowest ES distributions, demonstrating that such networks are more robust than the rest of networks, in the case of an epidemic-like failure with epidemic intensity $s = 3$.

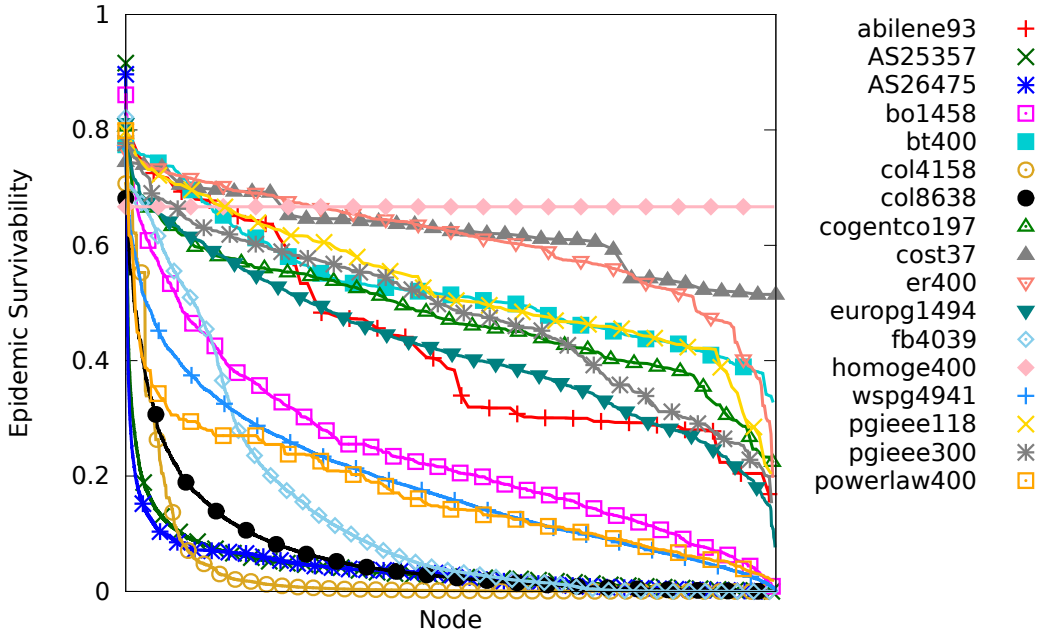


Fig. 3. *Epidemic survivability* distribution, sorted from major to minor values, of all networks. In this case the set of parameters has been: $s = 3$, $\delta = 0.3$, $k = 2000$ and $tol = 1e^{-8}$. The X-axis shows the nodes of the network, their index not showed for the sake of clarity.

It is worth noting that different types of complex networks show different ES distribution curves. While AS and collaboration networks show power-law-like curves, power grids, telecommunication networks, synthetic networks and the biological network depict more smooth-decreasing curves. On one hand, curves showing a rapid decrease (i.e. power-law-like profile) would be expected in complex networks regarding critical infrastructures. This is due to the fact that only a small portion of the nodes of the network would be highly vulnerable, and consequently, it would require less effort (e.g. economical) from the network engineer or operator to protect it. On the other hand, regarding social networks one could expect different curve profiles, depending on the purpose of the social network (e.g. a country's government interested in controlling its social networks would prefer flatter curves, because there would not be any node with a high spreading potential).

IV. Cascading failures

A cascading failure event is typically triggered by a single point of failure (i.e. one component) that leads to a domino effect, causing other parts of the network to fail. When such failures occur they can affect significant percentages of the world's population. For instance, according to [38], in 2012 a cascading failure in North India left more than 300 million people without power.

Cascading failure models have been used to understand these dynamic multiple failures in different types of complex networks. The power grids are the most remarkable example where cascading failures can occur. There

are several works which have studied the impact of cascading failures on different power grids: Italy [39], North America [40] and Europe [41]. However, cascading failures are not limited to power grids, but any load/capacity related complex network. For example, the authors of [42] stated that two types of cascading failures can occur in backbone telecommunication networks. Other works such as [43] and [44] have focused on the IP layer and optical layer of communication networks, respectively. Moreover, cascading failures have been also studied in socio-technological networks [45]. Other examples of cascading failures include biological, electronic and financial networks.

Although the authors of [46] proposed a robustness metric for power grid networks in the case of targeted attacks, to the best of our knowledge, there is not any metric which can be generally applied to any kind of cascading failure or complex network. Therefore, with the purpose of providing the network scientific community with such a measure, in this section we define *cascading survivability*.

A. Cascading Failure Models

Cascading failures have been extensively studied in the literature. Some of the most well-known models are presented next. In [47] one of the first cascading failure models was presented, which focused on random complex networks. Contemporarily, the authors of [48] presented a simple but functional model. Later on, the model was enhanced in [49] by keeping an auxiliary cost matrix related with the efficiency metric [50], [51]. Furthermore, in [52] the authors proposed an analytically tractable loading-dependent cascading failure model. In [53] an AC blackout model representing most of the interactions observed in cascading failures was presented. Recently, in [54] a cascading failure model for inter-domain routing systems was presented. Moreover, the authors proposed two metrics to assess the impact of a cascading failure: the proportion of failure nodes and the proportion of failed links.

As previously stated in this work, our objective is to define a metric able to characterize the vulnerability of the elements of a network (i.e. in this case nodes) under cascading failures. To do so, we have chosen the model presented in [48]. According to this model, each node j is related with a load L_j. The load at each node is the node betweenness centrality, i.e. the number of shortest paths passing through the node. Then, the capacity can be defined as a proportional value to the initial load L_j, as denoted by Eq. 5:

$$C_j = (1+\alpha)\cdot L_j \qquad j = 1, 2, \ldots, N \tag{5}$$

where N is the number of nodes of the network and α, the *tolerance* parameter of the model, is a constant that must be $\alpha \geq 0$. This parameter is related with the concept of *capacity dimensioning* of a network, which is of paramount importance at the designing phase of a network (e.g. a critical infrastructure such as a power grid). An appropriate level of *over-dimensioning* can prevent a network from cascading failures. However, a higher α typically involves a higher economical budget. Therefore, network engineers must seek a trade-off between these two factors.

As defined by the model in [48], we focus on cascades triggered by the removal of a single node. This event, in general, causes changes in the distribution of shortest paths. As a result, after an initial node failure, the new load

of the nodes (L'_j) might be different from the initial load (L_j). Then, for each node, if the expression of Eq. 6 is satisfied:

$$L'_j > C_j \tag{6}$$

the node j overloads and fails, which might cause subsequent overloading failures on the rest of nodes of the network.

Finally, we note that in the results presented further in this section we have assumed an $\alpha = 0.05$ for all networks, with the purpose of allowing comparison among them.

B. Cascading Survivability

Our new network measure called *cascading survivability* (CS) is presented below. *Cascading survivability* evaluates how potentially injurious a node is according to a specific cascading failure scenario. In other words, CS can be described as shown in Eq. 7:

$$CS_i(\alpha) = \frac{\text{the number of nodes that fail if node } i \text{ initially fails}}{\text{all nodes in the network} - 1} \qquad 1 = 1, \ldots, N \tag{7}$$

where N is the number of nodes of the network. As observed, α is a parameter of CS, what means that for different α distinct CS values might be obtained. *Cascading survivability* takes values in the range between 0 and 1 for each node, where higher the value, more harmful is the node under a specific cascading failure scenario.

We have defined a procedure to compute the *cascading survivability* of the nodes of a network, which is presented in Algorithm 2. As shown, the method requires two parameters: the network $\mathcal{G}$ and the tolerance parameter α. First of all, the initial load and capacity of each node is computed (lines 4 to 7). Then, an initial failure is caused, for each one of the nodes of the given network, one at a time (lines 8 to 20). For each initial failure (line 9) and as well as at each step of the spreading of the cascade, (lines 10 to 19), the new load of the remaining nodes of the network is computed (line 13). If the new load becomes higher than the capacity at any step, then the *cascading survivability* of the node that initially triggered the failure is increased (lines 14 to 17). Finally, the CS of each node is normalized (lines 21 to 23).

C. The distribution

When computing the *cascading survivability* for the nodes of a network, given a network and a specific α, it is worth noting the utility of analysing the distribution of the CS values, as previously illustrated for *epidemic survivability* in Section III-C.

By sorting the CS values in descending order it is possible to compare different networks, according to a specific cascading failure scenario denoted by α. Fig. 4 shows the CS distribution of 15 of the networks considered in this work, in the case of a cascading failure with $\alpha = 0.05$. It is interesting to note that most of the networks show a bimodal CS distribution. This means that the nodes of such networks can be clearly divided in two groups: *harmful* and *not significant* in the case of a cascading failure. This behavior has been observed in other works such as [55].

Algorithm 2 Compute *cascading survivability*.

Require: $\alpha \geq 0, connected\ \mathcal{G}$

Input: a graph $\mathcal{G}$ and the constant α (tolerance parameter).
Output: an array containing the *cascading survivability* of each node.
$N \leftarrow$ vertexSize($\mathcal{G}$))
{initializing load and capacity of each node}
for all $v \in vertexSet(\mathcal{G})$ **do**
    $L[v] =$ NodeBetweennessCentrality($\mathcal{G}$)
    $C[v] = (1 + \alpha) \cdot L[v]$
end for
for all $v \in vertexSet(\mathcal{G})$ **do**
    $F \leftarrow$ add(v) {add node v to the list of nodes that are going to fail}
    while F is not empty **do**
        $\mathcal{G}' \leftarrow$ removeNodes($\mathcal{G}$,F) {removes from $\mathcal{G}$ all nodes in F. After the operation F is empty.}
        for all $u \in vertexSet(\mathcal{G}')$ **do**
            $L'[u] =$ NodeBetweennessCentrality($\mathcal{G}'$)
            if $L'[u] > C[u]$ **then**
                $F \leftarrow$ add(u)
                $CS[v] = CS[v] + 1$ {increase in 1 the number of nodes that have failed due to the initial failure of v}
            end if
        end for
    end while
end for
for all $v \in vertexSet(\mathcal{G})$ **do**
    $CS[v] = \frac{CS[v]}{N-1}$
end for
return CS

Moreover, as observed, depending on the network the percentage of harmful nodes might vary. For instance, the *fb4039* and the *er400* networks start the distribution around 0.9, however it is in the former where only a 5% of the nodes represents a *threat* in the case of cascading failures, while in the latter it is about 55%. Finally, different types of complex networks show different CS distribution curves, just like they show different ES curves as represented in Section III-C.

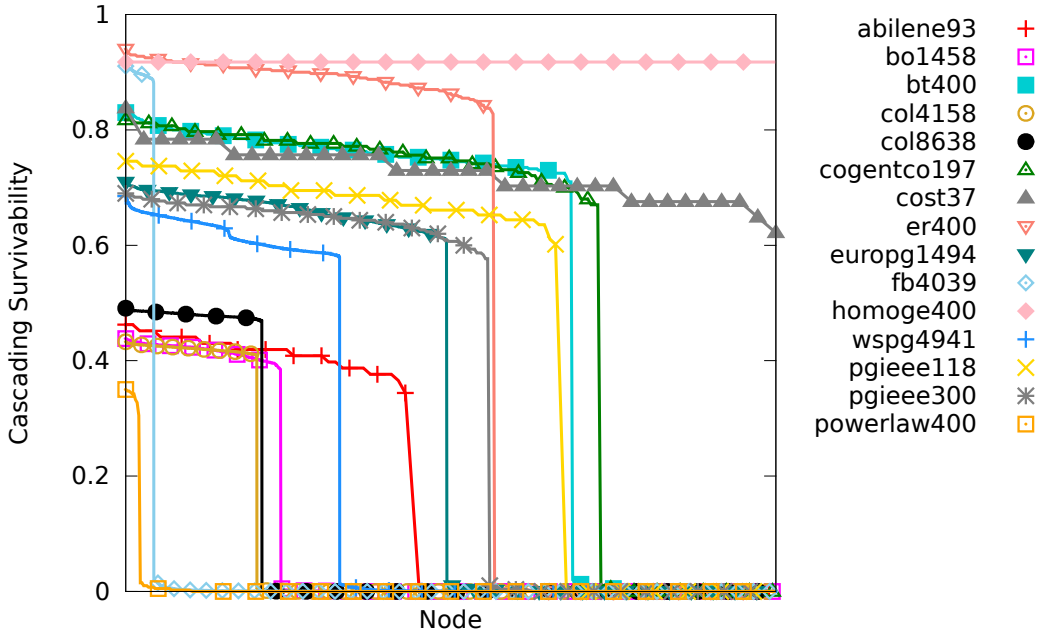


Fig. 4. *Cascading survivability* distribution, sorted from major to minor values, of all networks. In this case we have considered $alpha = 0.05$. The X-axis shows the nodes of the network, their index not showed for the sake of clarity.

V. Summary and Conclusions

In this paper we have proposed two new measures to evaluate the vulnerability of complex networks in two different dynamic multiple failure scenarios: epidemic-like and cascading failures.

Firstly, we have proposed a new network measure called *epidemic survivability* (ES), which describes the vulnerability of each node of a network under a specific epidemic-like failure propagation scenario. Besides, a procedure to compute our novel measure has been provided. Sorting the ES distribution of values of all nodes of a network in descending order, it is possible to analyze which nodes would be more vulnerable in the case of an epidemic failure. Furthermore, using this ES distribution, network vulnerability can be compared for a specific epidemic scenario.

Secondly, we have presented a new network measure called *cascading survivability* (CS), which characterizes how potentially dangerous a node is according to a specific cascading failure scenario. In addition, we have provided a procedure to compute CS. Then, as for the *epidemic survivability* metric, we have noted the inherent usability related to the CS distribution.

Lastly, we have computed ES and CS for the set of networks considered in this work, being each measure dependent on a specific failure scenario. Results have shown that distinct types of complex networks might react differently under the same dynamic multiple failure. In addition, results have revealed that a complex network might be more or less vulnerable, depending on the specific type of multiple failure scenario (i.e. epidemic-like

or cascading failures). For instance, while the *cogentco197* network shows a smooth decreasing curve of ES, the same network shows a bimodal distribution of CS, where about 25% of nodes are not dangerous in the case of cascading failures.

To conclude, the *methodology* that we have followed to evaluate the vulnerability of the nodes of a network in the case of dynamic multiple failures might be used in further investigations, considering other types of failures or models. This methodology is defined below:

1) Define the set of networks to be analysed.
2) Determine the failure scenario.
3) Choose a suitable model to simulate the failures.
4) Define the value of all the parameters of the model.
5) For each network, compute the vulnerability of the elements (e.g. nodes) of the network analytically or by performing simulations.

ACKNOWLEDGEMENTS

This work is partially supported by Spanish Ministry of Science and Innovation projects TEC 2012-32336 and MTM 2011-27739-C04-03, and by the Generalitat de Catalunya research support program SGR-1202. This work is also partially supported by the Secretariat for Universities and Research (SUR) and the Ministry of Economy and Knowledge through AGAUR FI-DGR 2012 and BE-DGR 2012 grants (M. M.)

REFERENCES

[1] Kun Yang, Xueqi Cheng, Liang Hu, and Jianming Zhang. Mobile social networks: state-of-the-art and a new vision. *International Journal of Communication Systems*, 25(10):1245–1259, 2012.

[2] http://www.dailyfinance.com/2013/08/14/apple-icahn-stock-rebound-value/. [Online; accessed 28-Sep-2013].

[3] James P.G. Sterbenz, David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, and Paul Smith. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8):1245–1265, 2010.

[4] M.M.A. Azim and A.M. El-semary. Vulnerability assessment for mission critical networks against region failures: A case study. In *Proceedings of the 2nd International Conference on Communications and Information Technology (ICCIT)*, 2012.

[5] M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, and D. Harle. Endurance: A new robustness measure for complex networks under multiple failure scenarios. *Computer Networks*, (0):–, 2013. in Press.

[6] Marc Manzano, Eusebi Calle, Jordi Ripoll, Anna Manolova Fagertun, and Víctor Torres-Padrosa. Epidemic survivability: Characterizing networks under epidemic-like failure propagation scenarios. In *Proceedings of the 9th International Conference on the Design of Reliable Communication Networks (DRCN)*, pages 95–102, 2013.

[7] P. Cholda, A. Jajszczyk, and K. Wajda. A unified quality of recovery (QoR) measure. *International Journal of Communication Systems*, 21(5):525–548, 2008.

[8] www.topology-zoo.org. [Online; accessed 28-Sep-2013].

[9] B. Bollobás. Random graphs. *Cambridge University Press*, 73, 2001.

[10] A. L. Barabasi and R. Albert. Emergence of scaling in random networks. *Science*, 286(5439):509–512, 1999.

[11] H. Jeong, S.P. Mason, A.L. Barabasi, and Z.N. Oltvai. Lethality and centrality in protein networks. *Nature*, 411:41–42, 2001.

[12] Jure Leskovec, Jon Kleinberg, and Christos Faloutsos. Graph evolution: Densification and shrinking diameters. *ACM Transactions on Knowledge Discovery from Data*, 1(1):2, 2007.

[13] Neil Hutcheon and Janusz W. Bialek. Updated and validated power flow model of the main continental european transmission network. In *Proceedings of the IEEE PowerTech 2013*, 2013.

[14] Julian J. McAuley and Jure Leskovec. Learning to discover social circles in ego networks. In *NIPS*, pages 548–556, 2012.

[15] Duncan J. Watts and Steven H. Strogatz. Collective dynamics of 'small-world' networks. *Nature*, 393(6684):440–442, 1998.

[16] University of Washington. http://www.ee.washington.edu/research/pstca/. [Online; accessed 28-Sep-2013].

[17] The DIMES project. http://www.netdimes.org/. [Online; accessed 28-Sep-2013].

[18] Stanford Network Analysis Project. http://snap.stanford.edu/. [Online; accessed 28-Sep-2013].

[19] M. E. J. Newman. The structure and function of complex networks. *SIAM Review*, 45:167–256, 2003.

[20] G. Marks and W.K. Beatty. *Epidemics*. Scribner, 1976.

[21] Pawel Kulakowski, Eusebi Calle, and José-Luis Marzo. Performance study of wireless sensor and actuator networks in forest fire scenarios. *International Journal of Communication Systems*, 26(4):515–529, 2013.

[22] Alison L. Hill, David G. Rand, Martin A. Nowak, and Nicholas A. Christakis. Emotions as infectious diseases in a large social network: the SISa model. *Proceedings of the Royal Society B: Biological Sciences*, 277(1701):3827–3835, 2010.

[23] Andrea Montanari and Amin Saberi. The spread of innovations in social networks. *Proceedings of the National Academy of Sciences*, 107(47):20196–20201, 2010.

[24] Bing-Hong Liu, Yu-Ping Hsu, and Wei-Chieh Ke. Virus infection control in online social networks based on probabilistic communities. *International Journal of Communication Systems*, 2013.

[25] E. Calle, J. Ripoll, J. Segovia, P. Vila, and M. Manzano. A multiple failure propagation model in GMPLS-based networks. *IEEE Network*, 24(6):17–22, 2010.

[26] M. Manzano, E. Calle, and D. Harle. Quantitative and qualitative network robustness analysis under different multiple failure scenarios. In *Proceedings of the 3rd IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 1–7, 2011.

[27] M. Manzano, J. L. Marzo, E. Calle, and A. Manolova. Robustness analysis of real network topologies under multiple failure scenarios. In *Proceedings of the 17th European Conference on Network and Optical Communications (NOC)*, 2012.

[28] M. Manzano, V. Torres-Padrosa, and E. Calle. Vulnerability of core networks under different epidemic attacks. In *Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, 2012.

[29] Romualdo Pastor-Satorras and Alessandro Vespignani. Epidemic spreading in scale-free networks. *Physical Review Letters*, 86(14):3200–3203, 2001.

[30] M. E. J. Newman. Spread of epidemic disease on networks. *Physical Review E*, 66:016128, 2002.

[31] Romualdo Pastor-Satorras and Alessandro Vespignani. Epidemic dynamics in finite size scale-free networks. *Physical Review E*, 65:035108, 2002.

[32] M. Boguñá and R. Pastor-Satorras. Epidemic Spreading in correlated complex networks. *Physical Review E*, 66:047104, 2002.

[33] Deepayan Chakrabarti, Yang Wang, Chenxi Wang, Jurij Leskovec, and Christos Faloutsos. Epidemic thresholds in real networks. *ACM Transactions on Information and System Security*, 10(4):1–26, 2008.

[34] T.G. Lewis. *Network Science: Theory and Applications*. Wiley, 2009.

[35] Mark E. J. Newman. *Networks: An Introduction*. Oxford University Press, 2010.

[36] R. Cohen and S. Havlin. *Complex Networks: Structure, Robustness and Function*. Cambridge University Press, 2010.

[37] Y. M. Ko and N. Gautam. Epidemic-based information dissemination in wireless mobile sensor networks. *IEEE/ACM Transactions on Networking*, 18(6):1738–1751, 2010.

[38] The Hindu. http://www.thehindu.com/news/national/article3702075.ece?homepage=true. [Online; accessed 28-Sep-2013].

[39] Paolo Crucitti, Vito Latora, and Massimo Marchiori. A topological analysis of the italian electric power grid. *Physica A: Statistical Mechanics and its Applications*, 338(1):92–97, 2004.

[40] Réka Albert, István Albert, and Gary L. Nakarado. Structural vulnerability of the North American power grid. *Physical Review E*, 69(2):025103+, 2004.

[41] Martí Rosas-Casals, Sergi Valverde, and Ricard V. Solé. Topological vulnerability of the european power grid under errors and attacks. *International Journal of Bifurcation and Chaos*, 17(7):2465–2475, 2007.

[42] M. Farhan Habib, Massimo Tornatore, Ferhat Dikbiyik, and Biswanath Mukherjee. Disaster survivability in optical communication networks. *Computer Communications*, 36(6):630–644, 2013.

[43] E.G. Coffman Jr, Z. Ge, Vishal Misra, and Don Towsley. Network resilience: Exploring cascading failures within BGP. In *Proceedings of the 40th Annual Allerton Conference on Communication, Control and Computing*, 2002.

[44] Ridha Rejeb, 1963-Leeson Mark S., and Roger J. Green. Fault and attack management in all-optical networks. *IEEE Communications Magazine*, 44(11):79–86, November 2006.

[45] Chris Barrett, Karthik Channakeshava, Fei Huang, Junwhan Kim, Achla Marathe, Madhav V. Marathe, Guanhong Pei, Sudip Saha, Balaaji S. P. Subbiah, and Anil Kumar S. Vullikanti. Human initiated cascading failures in societal infrastructures. *PLoS ONE*, 7(10):e45406, 2012.

[46] Yakup Koç, Martijn Warnier, Frances M. T. Brazier, and Robert E. Kooij. A robustness metric for cascading failures by targeted attacks in power networks. In *Proceedings of the 10th IEEE International Conference on Networking, Sensing and Control*, 2013.

[47] Duncan J. Watts. A simple model of global cascades on random networks. *Proceedings of the National Academy of Sciences*, 99(9):5766–5771, 2002.

[48] Adilson E. Motter and Ying C. Lai. Cascade-based attacks on complex networks. *Physical Review E*, 66(6):065102+, 2002.

[49] Paolo Crucitti, Vito Latora, and Massimo Marchiori. Model for cascading failures in complex networks. *Physical Review E*, 69:045104, 2004.

[50] Vito Latora and Massimo Marchiori. Efficient behavior of small-world networks. *Physical Review Letters*, 87(19):198701, 2001.

[51] Y.-C. Lai, A.E. Motter, and T. Nishikawa. *Lecture Notes in Physics*, page 299.

[52] Ian Dobson, Benjamin A. Carreras, and David E. Newman. A loading-dependent model of probabilistic cascading failure. *Probability in the Engineering and Informational Sciences*, 19:15–32, 1 2005.

[53] Dusko P. Nedic, Ian Dobson, Daniel S. Kirschen, Benjamin A. Carreras, and Vickie E. Lynch. Criticality in a cascading failure blackout model. *International Journal of Electrical Power and Energy Systems*, 28(9):627–633, 2006.

[54] Yi Guo, Zhenxing Wang, Shaopeng Luo, and Yu Wang. A cascading failure model for interdomain routing system. *International Journal of Communication Systems*, 25(8):1068–1076, 2012.

[55] Sakshi Pahwa, Amelia Hodges, Caterina M. Scoglio, and Sean Wood. Topological analysis of the power grid and mitigation strategies against cascading failures. *CoRR*, abs/1006.4627, 2010.

C Selected conference publications

Manzano, M., Calle, E., Ripoll, J., Fagertun, A.M., Torres-Padrosa, V. “Epidemic survivability: Characterizing networks under epidemic-like failure propagation scenarios”, in *9th International Conference on the Design of reliable communication networks (DRCN)*, March 4-7, 2013, Budapest. Budapest: IEEE, 2013. pp: 95-102

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6529887

ABSTRACT

Epidemics theory has been used in different contexts in order to describe the propagation of diseases, human interactions or natural phenomena. In computer science, virus spreading has been also characterized using epidemic models. Although in the past the use of epidemic models in telecommunication networks has not been extensively considered, nowadays, with the increasing computation capacity and complexity of operating systems of modern network devices (routers, switches, etc.), the study of possible epidemic-like failure scenarios must be taken into account. When epidemics occur, such as in other multiple failure scenarios, identifying the level of vulnerability offered by a network is one of the main challenges. In this paper, we present epidemic survivability, a new network measure that describes the vulnerability of each node of a network under a specific epidemic intensity. Moreover, this metric is able to identify the set of nodes which are more vulnerable under an epidemic attack. In addition, two applications of epidemic survivability are provided. First, we introduce epidemic criticality, a novel robustness metric for epidemic failure scenarios. A case study shows the utility of this new metric comparing several network topologies and epidemic intensities. Then, two immunization strategies are proposed: high epidemic survivability (HES) and high epidemic survivability adaptive (HESA). The presented results show that network vulnerability can be significantly reduced by using our proposals, compared to other well-known existing methods.

KEYWORDS

- Epidemics
- Immunization
- Multiple Failures
- Network Characterization
- Robustness Metrics

2012 11th Annual Workshop on Network and Systems Support for Games

NetGames 2012

Venice, Italy

November 22-23, 2012

IEEE Catalog Number CFP1276I-ART

ISBN 978-1-4673-4578-1

M. Manzano, Henández J.A., M. Urueña, E. Calle. “An empirical study of cloud gaming”, 11th Annual Workshop on Network and Systems Support for Games (NetGames), Nov. 22-23, 2012, Venice. Venice: IEEE, 2012. pp.: 1-2

http://dx.doi.org/10.1109/NetGames.2012.6404021

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6404021

ABSTRACT

Online gaming connects players from all over the world together for fun and entertainment, and has been regarded as one of the most profitable and popular Internet services. Besides, there is a growing trend towards moving local applications to remote data centers: this is often referred to as the cloud. With the purpose of studying the impact of Cloud Gaming on the access network load, in this paper we carry out an empirical network traffic analysis of two well-known cloud gaming platforms: On-Live and Gaikai. Traffic traces have been collected and analysed from five different games of both platforms. Cloud gaming has been observed to be remarkably different from traditional online gaming in terms of network load and traffic characteristics. Moreover, the traces have revealed similarities between the two platforms regarding the packet size distribution, and differences concerning the packet inter-arrival times. However, each platform shows a similar traffic pattern for most of the games it serves. Nonetheless, the racing and shooter games considered in this work demand more bandwidth than other game-genres.

KEYWORDS

- Bandwidth
- Cloud computing
- Educational institutions
- Games
- Graphics processing units
- Jitter
- Servers

IV International Congress on Ultra Modern Telecommunications and Control Systems 2012

IV International Congress on Ultra Modern Telecommunications and Control Systems 2012 took place 3-5 October 2012 in St. Petersburg, Russia.

Catalog number:	CFP1263G-ART
ISBN:	978-1-4673-2015-3

Spain); Ignacio Rodríguez (University of Valladolid, Spain); David Sánchez (University of Valladolid, Spain); Rubén M. Lorenzo (University of Valladolid, Spain); Ioannis Tomkos (AIT, Greece); Evaristo J. Abril (University of Valladolid, Spain)
pp. 793-799

A restoration scheme for virtual networks using switches
Son Pham (University of Technology of Compiègne & France Télécom, France); Jacques Carlier (Université de Technologie de Compiègne, France); Joël Lattmann (France Telecom, France); Jean-Luc Lutton (Orange Labs, France); Dritan Nace (Compiegne University of Technology, France); Laurent Valeyre (France Telecom, France)
pp. 800-805

T17: Power Systems

Open Multi-technology Building Energy Management System
Jaime Caffarel (Universidad Politecnica de Madrid, Spain); Guillermo del Campo-Jimenez (Universidad Politécnica de Madrid, Spain); Jorge M. Perandones (Universidad Politécnica de Madrid & CeDInt, Spain); César Gomez-Otero (Technical University of Madrid & CeDInt-UPM, Spain); Rocio Martínez (Universidad Politécnica de Madrid, Spain); Asunción Santamaría (Universidad Politécnica de Madrid, Spain)
pp. 397-404

Wired Smart Home: energy metering, security, and emergency issues
Manfred Schneps-Schneppe (Ventspils University College, Latvia); Anatoly Maximenko (National Research University of Electronic Technology, Russia); Dmitry Namiot (Moscow State University, Russia); Dmitry Malov (Zelenograd Center for Innovation and Technology, Russia)
pp. 405-410

Current Interoperability of Electrical Systems
Luis de Andrade (Faculdade de Engenheria da Universidade do Porto, Portugal); Teresa Ponce de Leão (Laboratório Nacional de Energia e Geologia, Portugal)
pp. 411-418

T18: PHY & Channels III

Universal algorithm for demodulating multi-position PSK signals
Alexey Loginov (Nizhny Novgorod State University (NNSU), Russia); Dmitry Marychev (Nizhny Novgorod State University (NNSU), Russia)
pp. 419-422

Use of Predistortion in Data Transmission Modems on Multipath Communication Channels
Alexander Malyutin (JCK Sozvezdie, Russia); Inna Dvorakova (Voronezh State University, Russia); Nechaev Yuri (Voronezh State University, Russia)
pp. 423-430

The detector's output SNR as a criterion for receiver placement in MIMO DVB-T based Passive Coherent Location
Mohammad Chitgarha (Sharif University of Technology, Iran); Mojtaba Radmard (Sharif University of Technology, Iran); Mohammad Nazari Majd (Sharif University of Technology, Iran); Babak Hossein Khalaj (Sharif University of Technology, Iran); Mohammad Mahdi Nayebi (Sharif University of Technology, Iran)
pp. 431-435

M. Manzano, V. Torres-Padrosa, E. Calle. “Vulnerability of core networks under different epidemic attacks”, 4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMTs), Oct. 3.-5, 2012, St. Petersburg. St. Petersburg: IEEE, 2012. pp.: 820-826

http://dx.doi.org/10.1109/ICUMT.2012.6459776

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6459776

ABSTRACT

This paper is focused on the propagation of failures within a core telecommunication network (i.e. virus or malicious code spreading), which are commonly represented using epidemic models. This work conducts an analysis of the vulnerability of five core telecommunication networks subject to different epidemic attacks. The difference between the attacks relies on the method used to select the initial set of infected nodes. As a novelty, the investigation is focused on the initial stage of the epidemics (first 48 hours). The analysis is carried out taking into account the topological connectivity of the networks. Results are presented in two phases. The first one concerns the first 24 hours of the epidemics evolution and shows the reaction of core networks to different types of epidemic attacks. The second one is focused on the time frame between 24 and 48 hours and presents a study of the repairing times needed to eradicate the epidemics. Results show that the core telecommunication networks react differently depending on the type of epidemics. Thus, different repairing times need to be applied in order to maintain a specific level of connectivity of the networks.

KEYWORDS

- Eigenvalues and eigenfunctions
- Indexes
- Network topology
- Telecommunication network reliability
- Topology

IEEE

IEEE COMMUNICATIONS SOCIETY

NOC OCSI 2012

17th European Conference on Network and Optical Communications
7th Conference on Optical Cabling and Infrastructure

June 20-22 2012
Vilanova i la Geltrú
Catalonia, Spain

Organized by

UPC

CRAAX

Technical Sponsors

IEEE

IEEE COMMUNICATIONS SOCIETY

Local Sponsors

Generalitat de Catalunya

neàpolis

i2cat

CANDA

TS6: Advances in Networking (Invited)

Empirical study based on Machine Learning Approach to Assess the QoS/QoE correlation
Sajid Mushtaq, Abdelhamid Mellouk, Brice Augustin, Emna Rekik

Total Cost Comparison of Next Generation Optical Access Networks with Node Consolidation
Carmen Mas Machuca, Kun Wang, Mario Kind, Koen Casier

Robustness Analysis of Real Network Topologies under Multiple Failure Scenarios
M.Manzano, Josep Lluís Marzo, Eusebi Calle, Anna Manolova

Using an Analytical Power Model to Survey Power Saving Approaches in Backbone Networks
Ward Van Heddeghem, Michael C.Parker, Sofie Lambert, Willem Vereecken, Bart Lannoo, Didier Colle, Mario Pickavet, Piet Demeester

Scalability Analysis of WSS-based ROADMs
Gianluigi Notarnicola, Giuseppe Rizzelli, Guido Maier, Achille Pattavina

TS7: Optical Networks II (Routing & Protection)

FRA: A New Fuzzy-based Routing Approach for Optical Transport Networks
Ehsan Ahvar, Eva Marín-Tordera, Marcelo Yannuzzi, Xavier Masip-Bruin, Shohreh Ahvar

Design of Virtual Optical Bus Networks: A Heuristic Approach
Ahmad Rostami, Sandeep Kumar Singh

Impairment-Aware Routing in Translucent Spectrum-Sliced Elastic Optical Path Networks
Song Yang, Fernando A. Kuipers

Improved Algorithm for Low Cost Lightpath Assignment in Mixed Line Rates WDM Networks
Dusan Skovajsa, Alejandra Beghelli

Rapid Protection Schemes in an All-Optical Packet Metro Ring
Lida Sadeghioon, Annie Gravey, Philippe Gravey

Building an MPLS-TP Simulator
Vishal Negi, Umang Kumar, Tulika Pandey, Ashwin A Gumaste

TS8: Network Performance

How Well Are we handling Electronic-Waste?
David W. Faulkner, Climate Associates Ltd

On the Effectiveness of Optical Parallel Transmission in IP Offloading
Xiaomin Chen, Mohit Chamania, Admela Jukan

Design, Deployment and Experimental Assessment of All-Optical Wavelength Conversion in the GMPLS-controlled ADRENALINE Testbed
Francisco Javier Vílchez, Raul Muñoz, Ramon Casellas, Ricardo Martinez, Ricard Vilalta

On Relay Selection for Cooperative Free-Space Optical Communication
Yasin Çelik, Niyazi Odabasioglu

GPON and EP2P: A Techno-Economic Study
Sergio Ricciardi, Germán Santos-Boada, Davide Careglio, Jordi Domingo-Pascual

Multilayer Restoration in Hierarchical IP/MPLS Over WSON Networks
Fernando Muñoz, Victor Lopez, Oscar González de Dios, Juan P. Fernández-Palacios

M. Manzano, J.L. Marzo, E. Calle, A. Manolova. “Robustness analysis of real network topologies under multiple failure scenarios”, 17th European Conference on Networks and Optical Communications (NOC), June 20-22, 2012, Vilanova i la Geltrú. Vilanova i la Geltrú: IEEE, 2012. pp.: 1-6

http://dx.doi.org/10.1109/NOC.2012.6249941

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6249941

ABSTRACT

Nowadays the ubiquity of telecommunication networks, which underpin and fulfill key aspects of modern day living, is taken for granted. Significant large-scale failures have occurred in the last years affecting telecommunication networks. Traditionally, network robustness analysis has been focused on topological characteristics. Recently approaches also consider the services supported by such networks. In this paper we carry out a robustness analysis of five real backbone telecommunication networks under defined multiple failure scenarios, taking into account the consequences of the loss of established connections. Results show which networks are more robust in response to a specific type of failure.

KEYWORDS

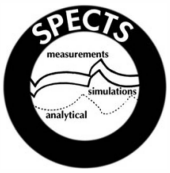
- Eigenvalues and eigenfunctions
- Laplace equations
- Measurement
- Network topology
- Robustness
- Topology

Proceedings of the 2012

International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS '12)

Mohammad Obaidat
Jose L. Sevillano
Pere Vila
Isaac Woungang
Raffaele Bolla
Daniel Cascado

Editors



Part of SummerSim 2012 Multiconference
July 8-11, 2012 Genoa, Italy
SIMULATION SERIES

ISBN: 978-1-61839-982-3
Volume 44 Book 12
IEEE Catalog Number: CFP1274E-ART
IEEE Catalog Number (CD-ROM version): CFP1274E-CDR

M. Manzano, J. Segovia, E. Calle, J.L. Marzo. “PHISON: Playground for High-level Simulations On Network”, 2012 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), June 8-11, 2012, Genoa, Italy. Genoa: IEEE, 2012. pp.: 1-6

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6267046&tag=1

ABSTRACT

Network simulation has become crucial in the study of telecommunication networks. In this paper we present PHISON (Playground for High-level Simulations On Networks), an easy-to-use discrete-event simulator whose features facilitate the study of diverse phenomena on path-oriented telecommunication networks (i.e. based on connections). A key differentiation feature of PHISON is that it considers the dynamic aspects of such networks at a higher level than previous proposals. Hence, our proposal does not consider protocol data units nor user data packets. Its design considerations and implementation details are presented and, finally, two examples illustrate some of the functionalities of the network simulator.

KEYWORDS

- Java
- Libraries
- Licenses
- Measurement
- Routing
- Topology

Bibliography

[BA99] A. L. Barabasi and R. Albert. Emergence of scaling in random networks. *Science*, 286(5439):509–512, 1999.

[BKM+14] K. Bilal, S. U. Khan, M. Manzano, E. Calle, S. A. Madani, K. Hayat, D. Chen, L. Wang, and R. Ranjan. Modeling and simulation of data center networks. In S. U. Khan and A. Y. Zomaya, editors, *Handbook on Data Centers*. Springer-Verlag, New York, USA, 2014.

[BMC+13] K. Bilal, M. Manzano, E. Calle, C. Scoglio, and S. U. Khan. Robustness Quantification of Hierarchical Complex Networks under Targeted Attacks. 2013. Submitted to Physica A.

[BMK+13] K. Bilal, M. Manzano, S.U. Khan, E. Calle, Keqin Li, and A.Y. Zomaya. On the characterization of the structural robustness of data center networks. *IEEE Transactions on Cloud Computing*, 1(1):1–1, 2013.

[Bol01] B. Bollobás. Random graphs. *Cambridge University Press*, 73, 2001.

[CMM12] E. Calle, M. Manzano, and J. L. Marzo. Multiple failures in telecommunication networks: robustness metrics and simulation tools. In *proceedings of the 2nd Workshop of Future Internet: Efficiency in high-speed networks (W-FIERRO 2012)*, 2012.

[CRS+10] E. Calle, J. Ripoll, J. Segovia, P. Vila, and M. Manzano. A multiple failure propagation model in gmpls-based networks. *IEEE Network*, 24(6):17–22, 2010.

[Lew09] Ted G. Lewis. *Network Science: Theory and Applications*. Wiley Publishing, 2009.

[Man09] M. Manzano. Entorn de simulació de fallades per a xarxes òptiques de transport. *Final project of Computer Science Engineering Bachelor (3rd-year), University of Girona*, 2009.

[Man11] M. Manzano. Metrics to evaluate network robustness in telecommunications networks. *Final project of Computer Science Engineering Bachelor (5th-year), University of Girona & Strathclyde University*, 2011.

[Man12] M. Manzano. New Robustness Evaluation Mechanisms for Telecommunication Network Topologies. *Master's Thesis, University of Girona*, 2012.

[MBCK13] M. Manzano, K. Bilal, E. Calle, and S.U. Khan. On the connectivity of data center networks. *IEEE Communications Letters*, 17(11):2172–2175, 2013.

[MCH11] M. Manzano, E. Calle, and D. Harle. Quantitative and qualitative network robustness analysis under different multiple failure scenarios. In *proceedings of the 3rd IEEE/IFIP International Workshop on Reliable Networks Design and Modelling (RNDM)*, 2011.

[MCR+13] M. Manzano, E. Calle, J. Ripoll, A. Manolova Fagertun, and V. Torres-Padrosa. Epidemic Survivability: Characterizing Networks Under Epidemic-like Failure Propagation Scenarios. In *proceedings of the 9th International Conference on Design of Reliable Communication Networks (DRCN)*, 2013.

[MCR+14] M. Manzano, E. Calle, J. Ripoll, A. Manolova Fagertun, V. Torres-Padrosa, S. Pahwa, and C. Scoglio. Epidemic and Cascading Survivability of Complex Networkss. *ArXiv e-prints 1405.0455*, 2014. Submitted to International Journal of Communications, Network and System Sciences.

[MCTP+13] M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, and D. Harle. Endurance: A new robustness measure for complex networks under multiple failure scenarios. *Computer Networks*, 57(17):3641–3653, 2013.

[MHUC12a] M. Manzano, J.A. Hernandez, M. Uruena, and E. Calle. An empirical study of cloud gaming. In *proceedings of the 11th Annual Workshop on Network and Systems Support for Games (NetGames)*, 2012.

[MHUC12b] M. Manzano, J.A. Hernandez, M. Uruena, and E. Calle. A first measurement study of online cloud gaming. In *proceedings of the 2nd Workshop of Future Internet: Efficiency in high-speed networks (W-FIERRO 2012)*, 2012.

[Mie11] Piet Van Mieghem. *Graph Spectra for Complex Networks*. 2011.

[MMCM12] M. Manzano, J.-L. Marzo, E. Calle, and A. Manolova. Robustness analysis of real network topologies under multiple failure scenarios. In *proceedings of the 17th European Conference on Networks and Optical Communications (NOC)*, 2012.

[MMR+14] M. Manzano, A. Manolova Fagertun, S. Ruepp, E. Calle, C. Scoglio, A. Sydney, A. de la Oliva, and A. Muñoz. Unveiling Potential Failure Propagation Scenarios in Core Transport Networks. *ArXiv e-prints 1402.2680*, 2014. Submitted to IEEE Communications Magazine.

[MRM14] A. Manolova Fagertun, S. Ruepp, and M. Manzano. Resolving epidemic network failures through differentiated repair times. *IET Networks*, 2014. Forthcoming.

[MSC+10] M. Manzano, J. Segovia, E. Calle, P. Vila, and J.-L. Marzo. Modelling spreading of failures in gmpls-based networks. In *proceedings of the 2010 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, 2010.

[MSCM12] M. Manzano, J. Segovia, E. Calle, and J. L. Marzo. PHISON: Playground for High-level Simulations On Networks. In *proceedings of the 2012 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, 2012.

[MSCV09] M. Manzano, J. Segovia, E. Calle, and P. Vila. Failure propagation models for gmpls-based networks. In *proceedings of the 2nd Workshop on Multilayer Networks: IP over Transport Networks*, 2009.

[MSS+14a] M. Manzano, F. Sahneh, C. Scoglio, E. Calle, and J. L. Marzo. Robustness surfaces: a universal measure for complex networks. In *proceedings of the International School and Conference on Network Science (NetSci 2014)*, 2014.

[MSS+14b] M. Manzano, F. Sahneh, C. Scoglio, E. Calle, and J. L. Marzo. Robustness surfaces of complex networks. *ArXiv e-prints 1404.2403*, 2014. Submitted to Scientific Reports.

[MTPC12] M. Manzano, V. Torres-Padrosa, and E. Calle. Vulnerability of core networks under different epidemic attacks. In *proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modelling (RNDM)*, 2012.

[MUS+14] M. Manzano, M. Urueña, M. Sužnjević, E. Calle, J.A. Hernández, and M. Matijasevic. Dissecting the protocol and network traffic of the onlive cloud gaming platform. *Multimedia Systems*, 2014. Forthcoming.

[RMC14] J. Ripoll, M. Manzano, and E. Calle. Spread of epidemic-like failures in telecommunication networks. *Physica A*, 410:457–469, 2014.

[SCH+10] I. Seoane, E. Calle, J.A. Hernández, J. Segovia, R. Romeral, P. Vilà, M. Urueña, and M. Manzano. A CTMC-based characterisation of the propagation of errors in GMPLS Optical Rings. In *proceedings of the 9th Workshop in GMPLS networks (WGN9)*, 2010.

[SCH+12] I. Seoane, E. Calle, J.A. Hernández, J. Segovia, R. Romeral, P. Vilà, M. Urueña, and M. Manzano. Failure propagation in gmpls optical rings: Ctmc model and performance analysis. *Optical Switching and Networking*, 9(1):39–51, 2012.

[SSYS10] A. Sydney, C. Scoglio, M. Youssef, and P. Schumm. Characterising the robustness of complex networks. *Int. J. Internet Technol. Secur. Syst.*, 2(3/4):291–320, 2010.

[Ste10] Maarten van Steen. *Graph theory and complex networks: an introduction*. 2010.

[TMCM13] V. Torres-Padrosa, M. Manzano, E. Calle, and J. L. Marzo. Community-based traffic preservation in telecommunication networks. *International Journal of Communication Systems*, 2013. Forthcoming.

[TPMCM12] V. Torres-Padrosa, M. Manzano, E. Calle, and J.-L. Marzo. Traffic-level community protection in telecommunication networks under large-scale failures. In *proceedings of the 2012 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, 2012.

[WS98] Duncan J. Watts and Steven H. Strogatz. Collective dynamics of 'small-world' networks. *Nature*, 393(6684):440–442, 1998.