ResiLyzer: A Tool for Resilience Analysis in Packet-Switched Communication Networks

David Hock, Michael Menth, Matthias Hartmann, Christian Schwartz, and David Stezenbach

University of Würzburg, Institute of Computer Science
Am Hubland, D-97074 Würzburg, Germany

Abstract. We present a tool for the analysis of fault-tolerance in packet-switched communication networks. Network elements like links or routers can fail or unexpected traffic surges may occur. They lead to service disruptions and degradations. Our tool quantifies these risks and presents a comprehensive digest of the results. We explain the core idea of the analysis and illustrate the tool.

1 Resilience Analysis

In previous work [1], we developed a framework for resilience analysis of packet-switched communication networks. Before we present the tool, we give a brief insight into the theoretical concept.

To analyze the resilience of a packet-switched communication network we require a model of the network's topology and the link bandwidths. The routing is known for the failure-free case and it can be computed for all possible failure cases. Further inputs are the expected traffic matrix as well as a probabilistic model for traffic surges h. Finally, a probabilistic model for link and router failures s is needed.

A networking scenario $z = (s, h)$ is characterized by a failure pattern s and traffic pattern h. An analysis of all possible networking scenarios is prohibitive because their number increases exponentially with the network size. Therefore, the most probable networking scenarios $\mathcal{Z}$ are identified and only they are used for the analysis. The selection process is controlled by a threshold p_{min} which controls the probability of the not-considered networking scenarios and provides error bounds on the obtained results.

In case of a network element failure, traffic can be rerouted which increases the relative load on the links of the backup paths. Such an increase can also be observed due to traffic surges. To analyze this effect, we calculate the distribution of the relative load for all links in the network by analyzing the relative link load for each considered networking scenario $z \in \mathcal{Z}$ and weighting these partial results with the probability of that networking scenario. If a network is physically partitioned by the failure of network elements or if the routing algorithm cannot provide a backup path, the network may be unavailable for some ingress-egress pairs. This unavailability is also calculated.

This analysis leads to extensive results which are hard to monitor. We use a complementary cumulative distribution function (CCDF) of the relative load per link. Furthermore, we propose to condense the information of the CCDF into a single value and use

This work is funded by Deutsche Forschungsgemeinschaft (DFG) under grant TR257/23-2. The authors alone are responsible for the content of the paper.

this value to color the corresponding link in the network graph. This allows to easily view the risk of overload in a network. The unavailability can be presented per ingress-egress pair, it can be aggregated per router, or it can be expressed relative to the overall traffic.

Further details and algorithms are available in [1]. In [2] we proposed additional illustrations to compare the potential overload for different routings.

2 ResiLyzer

The ResiLyzer has been developed to implement the presented concept into a software tool. An analysis with the ResiLyzer normally consists of four steps. First, the necessary input data is provided by loading existing topology, traffic matrix, and link cost files or creating new ones via the corresponding panels or menu bars. Second, the relevant networking scenarios including effective topologies and traffic matrices are configured. Third, the general analysis is invoked and the analytical results are computed. Fourth, the analytical results are interpreted by choosing one of the proposed comprehensive views or exporting the raw data for further analysis.

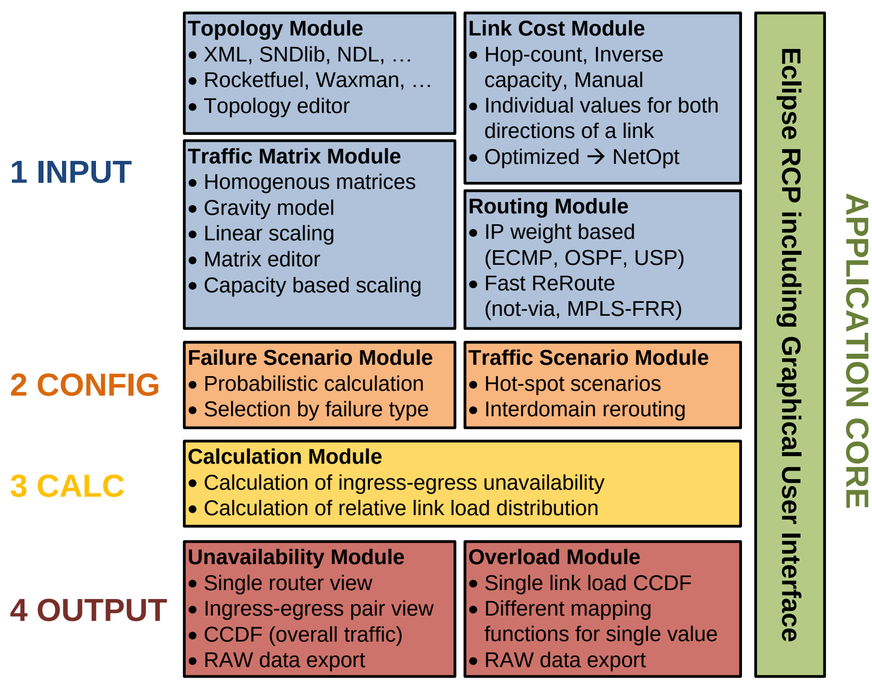

Fig. 1. Program structure of the ResiLyzer.

The ResiLyzer is implemented as an Eclipse RCP application. All elements of the tool are modular which makes them easily extensible. Figure 1 shows an overview of the program structure. Each module is displayed together with its main features that are currently implemented. The application core is formed by the Eclipse RCP application and the corresponding GUI. There are currently four input modules: modules for topologies, traffic matrices, link costs, and routing. The ResiLyzer has been equipped with a large collection of precalculated example scenarios including the Rocketfuel topologies [3] and a selection of random topologies created with the Waxman model [4]. These scenarios consist of the topologies, corresponding traffic matrices created with a simple gravity model [5], and link costs optimized with our NetOpt tool [6, 7]. The currently implemented routings of the ResiLyzer include ECMP, OSPF as well as Unique Shortest Path (USP) [8]. Additionally, several Fast ReRoute (FRR) mechanisms have been implemented.

The calculation of the considered networking scenarios z including failure scenarios s and traffic surges h is realized by special modules. Failure scenarios can be created either probabilistic with a threshold p_{min} or by selection of failure types, e.g., all single link and node failures. The currently supported types of traffic scenarios are hot-spot scenarios and interdomain rerouting scenarios.

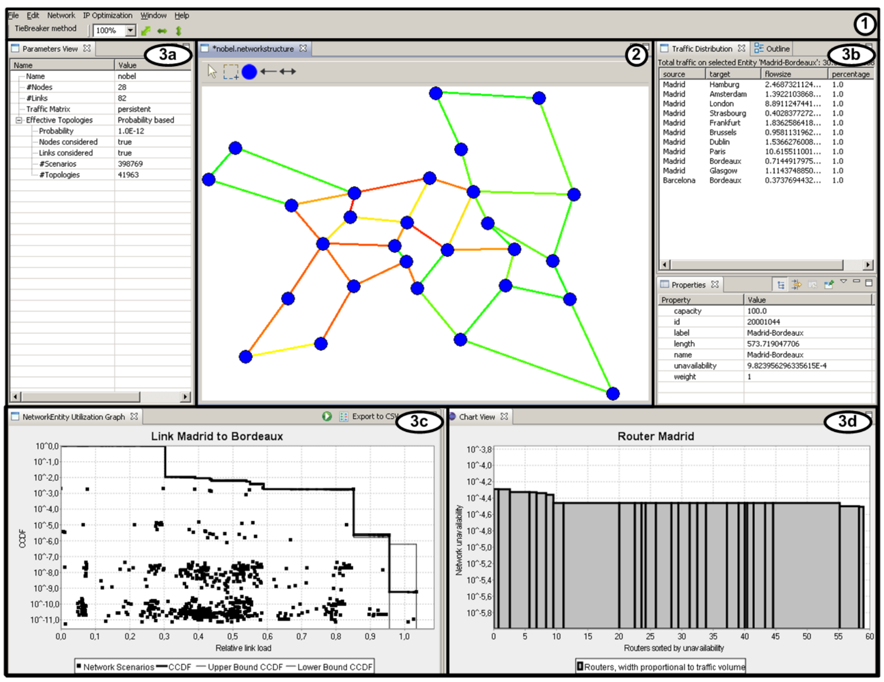

Fig. 2. Screenshot of the ResiLyzer.

The interpretation and illustration of the analytical results are performed by the unavailability and the overload module. Our tool offers different views and graphs to allow for a simple monitoring of fault-tolerance. The views can be activated and deactivated separately. The user can reach a certain view intuitively by selecting the corresponding element, e.g., links or failure scenarios. For instance, selecting a failure scenario shows the unavailability and load situation in the network in this failure scenario, selecting a link shows the relative link load of this link in all failure scenarios.

Figure 2 shows a screenshot of the ResiLyzer graphical user interface. It allows the user to highly adapt one's personal view on the tool, selecting the needed menus, panels, windows, etc. In the displayed example, a possible view configured for the analysis of the resilience data is shown. The menu (1) gives access to all functionality and also allows to toggle the different views. Area (2) contains a graph of the network topology. Depending on the current mode this topology graph can be displayed differently. In this case, the links are colored indicating the potential overload due to network failures. (3a) shows a summary of the input data and the values configured for the networking scenario computation. (3b) shows the properties of the link Madrid - Bordeaux and the traffic distribution on this link. (3c) contains a conditional CCDF of the relative link load for the same link together with a lower and an upper bound for the unconditioned CCDF. (3d) contains the network unavailability perceived by all aggregates of router Madrid. Further information about these graphs can be found in [1].

3 Conclusion

We presented the ResiLyzer, a tool for resilience analysis in packet-switched communication networks. The ResiLyzer offers a clear interface to input network data and calculates disconnection probabilities per ingress-egress pair and overload probabilities per link. In addition, it provides many options for the visualization of the computed results. Our approach defines a set of networking scenarios for the analysis whose size can be controlled by parameters so that the accuracy of the results can be traded for computation time.

Acknowledgments

The authors thank Prof. Phuoc Tran-Gia for the stimulating environment which was a prerequisite for this work.

References

1. Menth, M., Duelli, M., Martin, R., Milbrandt, J.: Resilience Analysis of Packet-Switched Communication Networks. accepted for IEEE/ACM Transactions on Networking (2010)
2. Hock, D., Hartmann, M., Schwartz, C., Menth, M.: Effectiveness of Link Cost Optimization for IP Rerouting and IP Fast Reroute. In: GI/ITG Conference on Measuring, Modelling and Evaluation of Computer and Communication Systems (MMB) and Dependability and Fault Tolerance (DFT), Essen, Germany (2010)
3. Spring, N., Mahajan, R., Wetherall, D., Anderson, T.: Measuring ISP Topologies with Rocketfuel. IEEE/ACM Transactions on Networking **12** (2004)
4. Zegura, E.W., Calvert, K.L., Donahoo, M.J.: A Quantitative Comparison of Graph-Based Models for Internet Topology. IEEE/ACM Transactions on Networking **5** (1997) 770–783
5. Medina, A., Taft, N., Salamatian, K., Bhattacharyya, S., Diot, C.: Traffic Matrix Estimation: Existing Techniques and New Directions. In: ACM SIGCOMM, Pittsburgh, USA (2002)
6. Menth, M., Hartmann, M., Martin, R.: Robust IP Link Costs for Multilayer Resilience. In: IFIP-TC6 Networking Conference (Networking), Atlanta, GA, USA (2007)
7. Hartmann, M., Hock, D., Schwartz, C., Menth, M.: Objective Functions for Optimization for Resilient and Non-Resilient IP Routing. In: 7^{th} International Workshop on Design of Reliable Communication Networks (DRCN), Washington, D.C., USA (2009)
8. Hock, D., Hartmann, M., Menth, M., Schwartz, C.: Optimizing Unique Shortest Paths for Resilient Routing and Fast Reroute in IP-Based Networks. In: IEEE Network Operations and Management Symposium (NOMS), Osaka, Japan (2010)