STSM report:
Evaluating and improving the robustness of the networks under attacks

Student: Petra Stojsavljevic Vizarreta
Host: Universidad de Girona (UdG), Spain
Home: Technical University of Munich (TUM), Germany
Supervisors: Jose Luis Marzo (UdG), Carmen Mas Machuca (TUM)
Working group: Malicious human activities (WG4)
Period: July 23, 2017 to July 29, 2017

July 31, 2017

1 Motivation

Malicious human activities, such as deliberate attacks on the central network elements or virus spreading can cause several damage to communication networks. A study on robustness of 15 real telecommunication networks by Rueda et al. [RCM17] showed that today's networks are not particularly robust to such kind of failures. Moreover, the critical services running over these networks typically rely on dedicated 1:1 or 1+1 protection which guarantees the service continuity in case of single link or node failures, but does not provide an adequate protection in the case of multiple failures, especially when the failures are geographically correlated. On another hand the restoration mechanisms triggered in the case of service interruptions may fail due to the lack of capacity, especially when the attacks are targeting the network elements with high betweenness centrality.

Network robustness metrics proposed so far relied only on the topological network features, such as average node degree, average two terminal reliability, and many others [VMDW+10, MCH11, MCSS+14] without considering how services are routed through the network and their corresponding fault prevention and fault mitigation strategies. However, in order to evaluate the real impact that the attack would have on the network service provider, we have to consider not only the topological features of the network, but also the service specific parameters as well as the limited network capacity. For instance, in the case of massive attack service between two endpoints might be lost a) due to the loss of the connectivity, b) lack of the network capacity to restore the connection over the alternative path or c) because the restored connection exceeds the minimum tolerable latency. Only the number connections due to the lack of connectivity may be predicted from the graph features (e.g. average two terminal reliability), while other two depend on the service QoS requirements and physical characteristics of the network.

Our goal is to propose **service robustness metric** that can reflect more accurately the performance of the network under attack. This service robustness metric can be used to quantify:

1. The improvement of the network topology hardening (e.g. the effect of installation of the additional link or additional capacity)
2. The efficiency of service protection schemes (e.g. compare different multipath strategies for survivable service routing)

1.1 Work progress during STSM

The research group of Broadband Communications and Distributed Systems at UdG has developed the simulator to evaluate the robustness of the networks under different multiple failure scenarios. During the STSM of Sergio Gomez from UdG at TUM, Sergio successfully integrated our traffic related robustness metrics and basic routing algorithm into the UdG simulator. The goal of my visit to UdG was to extend the basic routing algorithm (full restoration based on shortest paths), with more realistic routing strategies (partial restoration, dedicated protection), analyze the relationship of the traffic related metrics with the R* in the realistic telecommunication networks, provided by SNDlib [OWPT10]. We also included a case study on national backbone network provided by Deutsche Telekom.

Attacks considered in our study are:

- Random node or link attacks
- Targeted simultaneous
- Targeted sequential
- Epidemic-like attacks (e.g. virus spreading)

2 Service robustness metric

Service robustness metric is derived from network topology features and robustness metric related to service traffic going over the network. To combine topological features with survived traffic, we follow the same approach as described in [MCSS$^+$14], by using the weighted sum of several robustness related metrics, where the weights are obtained by PCA. For more details see the article [MCSS$^+$14].

2.1 Robustness metrics derived from network topology

The robustness metrics derived from network topology depends solely on the features of the underlying graph. The most relevant graph features describing the network robustness are listed in Table 1 [MCSS$^+$14].

Note that the functional metrics R[VMDW$^+$10] and R* [MCSS$^+$14] combine several structural and centrality features, by computing their weighted sum. While for computing R[VMDW$^+$10] the graph feature weights represent the importance of the particular graph feature for a particular service, the weights in R* [MCSS$^+$14] are derived from PCA.

Structural metrics	**Centrality metrics**	**Functional metrics**
Average node degree	Degree centrality	Elasticity
Average shortest path length	Eigenvector centrality	Endurance
Diameter	Closeness centrality	Quantitative robustness
Assortativity coefficient	Betweenness centrality	Qualitative robustness
Heterogenity	Cross-clique centrality	R-value
Efficiency	Spreaders	**R*-value**
Vertex connectivity		
Edge connectivity		
Cluster coefficient		
Symmetry ratio		
Largest eigenvalue		
Algebraic connectivity		
Natural connectivity		
Effective graph resistance		
Graph diversity		
Weighted spectrum		
Percolation limit		
Number of spanning trees		
Average two terminal reliability		
Viral conductance		

Table 1: Taxonomy of robustness metric as defined by Manzano et al.[MCSS$^+$14]

2.2 Robustness metric related to service traffic

The traffic related robustness metrics depend on how the services are initially routed (which again depends on the network capacity and service traffic steering policy) and fault mitigation strategy. The robustness metric related to the survived service traffic after the attack includes:

- The number and the throughput of survived connections
- The used (or complementary residual) network capacity

Simple restoration and 1:1 dedicated protection will serve as a benchmark service routing strategies.

2.2.1 Partial and full restoration

Network is described as a graph $G = (V, E)$, where V denotes the nodes of the network that can generate or switch the traffic, and E represents the communication links. The links (i,j) have a limited bandwidth C_{ij}. The flows in the traffic demand are described as $d = (s_d, t_d, c_d)$, where s_d and t_d denote the source and destination of the traffic demand, and c_d denotes the data rate of the flow. Binary variables $z_{ij,d}$ indicate if the edge (i, j) carries flow d, and x_d indicate if the flow d is accepted.

Initially, all the flows are routed along the shortest path between the source and destination. After the attack, we try to restore the connections so that the survived throughput is maximized, given the capacity constraints of the links. In full restoration scenario all traffic flows can be rerouted, while in the more realistic partial restoration scenario only the traffic flows affected by the failure will be flagged for restoration, while the unaffected flows follow their initial path. We noted that the performance between the full and partial restoration is significant only under stringent link capacity constraints.

The objective is to maximize the throughput of the survived flows, while minimizing the sum of each demand's path length. Small weight is assigned to the number of used links, to ensure shortest possible paths $\epsilon \ll 1$.

$$\max \sum_{d\in D} x_d c_d - \epsilon \sum_{ij\in E} \sum_{d\in D} z_{ij,d} c_d$$

Capacity and flow conservation constraint have to hold.

$$\sum_{d\in D} z_{ij,d} c_d \leq C_{ij}; \forall (i, j) \in E;$$

$$z_{ij,d} \leq x_d; \forall (i, j) \in E; \forall d \in D;$$

$$\sum_{ij\in E; i=n} z_{ij,d} - \sum_{ij\in E; j=n} z_{ij,d} = s_{n,d} x_d - t_{n,d} x_d; \forall n \in V; \forall d \in D;$$

We also prevent the flow split, by allowing at most one incoming and one outgoing link to be used by the same flow:

$$\sum_{ij\in E; j=n} z_{ij,d} \leq 1; \forall n \in V; \forall d \in D;$$

$$\sum_{ij\in E; i=n} z_{ij,d} \leq 1; \forall n \in V; \forall d \in D;$$

Where s_d and t_d are helper functions defined as:

$$s_d(t_d) = \begin{cases} 1, \text{if } n \text{ is a source (destination) of flow } d \\ 0, \text{otherwise} \end{cases}$$

The metrics that we obtain from this optimization are the survived throughput and link utilization:

$$Throughput = \sum_{d \in D} x_d c_d$$

$$LinkUtilization = \frac{1}{|E|} \sum_{d \in D} \sum_{ij \in E} z_{ij,d} c_d$$

2.2.2 Dedicated protection

Initially all traffic flows are provided with two node disjoint paths. After the attack the number and the throughput of the survived flows, and link utilization are calculated.

3 Ongoing work and future collaborations

The visit to research group of Broadband Communications and Distributed Systems at University of Girona triggered an interesting discussion in the areas of definition, analysis and applicability of service robustness metric. We plan to do a follow up over email and conference calls, and possible during one of the future STSMs.

The following conferences have been identified as suitable for publishing the results of our collaboration:

- Communication QoS, Reliability and Modeling (CQRM) Symposium at International Workshop on Software Aging and Rejuvenation (ICC)
- International Conference on Dependable Systems and Networks (DSN)
- Intl. Conference on Design of Reliable Communication Networks (DRCN)

References

[MCH11] Marc Manzano, Eusebi Calle, and David Harle. Quantitative and qualitative network robustness analysis under different multiple failure scenarios. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on*, pages 1–7. IEEE, 2011.

[MCSS$^+$14] Marc Manzano Castro, Faryad Sahneh, Caterina Scoglio, Eusebi Calle Ortega, and Josep Lluís Marzo i Lázaro. Robustness surfaces of complex networks. *Scientific Reports, 2014, núm. 4, P. 6133*, 2014.

[OWPT10] Sebastian Orlowski, Roland Wessäly, Michal Pióro, and Artur Tomaszewski. SNDlib 1.0survivable network design library. *Networks*, 55(3):276–286, 2010.

[RCM17] Diego F Rueda, Eusebi Calle, and Jose L Marzo. Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements. *Journal of Network and Systems Management*, 25(2):269–289, 2017.

[VMDW$^+$10] P Van Mieghem, C Doerr, H Wang, J Martin Hernandez, D Hutchison, M Karaliopoulos, and RE Kooij. A framework for computing topological network robustness. *Delft University of Technology, Report20101218*, 2010.