Vulnerability analysis of Complex Networks:

Software tools for the evaluation of stochastic and deterministic indicators of interconnected networks

In the framework of CRESCO project, we investigate how to understand, represent and predict the vulnerability of large technological networks (i.e. national power grids, telecommunication networks, …) in terms of Quality of Service (QoS) delivery and in terms of network reliability, availability and performances. We propose a modelling methodology to evaluate QoS and availability of service delivered by large technological interconnected networks. Networks are described by means of the delivered service, network topology and functional behavior, failure and repair mechanisms of network main elements/segments and interconnection with other networks. Then each network is represented by a convenient modeling technique, able to capture network technological features and realistic assumptions of elements/segments failure and recovery mechanisms. Each technique, supported by an adequate software tool, is to be selected inside a heterogeneous modeling framework composed by:¨

- **combinatorial methods** (i.e. **Reliability Block Diagrams**; Fault-trees (FT); **Network Reliability Analyzers**)- assuming that events to be represented are statistically independent.
- **State-space methods** (i.e. Markov chains, Generalised Stochastic Petri Nets; Coloured Stochastic Petri Nets; **Stochastic Activity Networks**) - relying on the specification of the whole set of possible states of the system and of the possible transitions among them.
- **Formal verification** to address, the problem of computing the **Maximum Guaranteed Flow in Communication Networks (MGF)**.
- **Simulators**, for evaluation of telecommunication network performances under load, connectivity and service.

The modelling and analysis technique here presented originated from the study of an actual breakdown scenario, namely, the mini black out of a main Telco node located in Rome that occurred on January 2004. A breakage of a metallic pipe, that carried cooling water of the air conditioning plant, caused the flooding of the floor under which cables of Telco devices were located. The fault reverberated on the quality of telecommunication services (both fix-to-fix and fix-to-mobile) in the whole Rome area. With reference to the above scenario, we focus on the service availability of the communication between two control centres of a Supervision, Control and Data Acquisition system of a power distribution grid. The availability of such a communication depends upon the availability of three interconnected networks which had a major role in the accident sequence. a) The Telco network that connects two control centres of the SCADA system, throughout a HDSL connection; b) the Telco emergency power supply, which feeds Telco network at different Telco sites and c) the public power distribution grid that provides the main power supply at the different Telco sites. Telco network is represented by a **Reliability Block Diagram (RBD)** with the realistic assumption of independent failure/repair of each network element/segment. The Telco emergency power supply, constituted by on-site backup batteries (for short and intermittent interruptions) and diesel generators (for longer-term interruptions) is represented by a **Stochastic Activity Networks (SAN)** , to account for the dependencies among events, such as starting times, duration times, failure and repair activities. The power distribution grid is analyzed by means of a **Network Reliability Analyzer (NRA)**.

THE TOOL NRA (NETWORK RELIABILITY ANALYSER)
The Tool NRA can be down loaded from
http://www.afs.enea.it/project/cresco/LA3cresco_sp32_unipmn
The network is a graph G=(V,E) where V is the set of nodes and E the set of arcs.
Arcs and nodes are binary entities (either up or down).
Given the network topology and the probability associated to the network elements,
The NRA tool provides:
- **Qualitative analysis:**
  - Minimal paths
  - Minimal cuts
- **Quantitative analysis:**
  - **Reliability and Unreliability functions**

The NRA tool implements and compares two network reliability algorithms:
- Minpath analysis
- Graph visiting algorithm

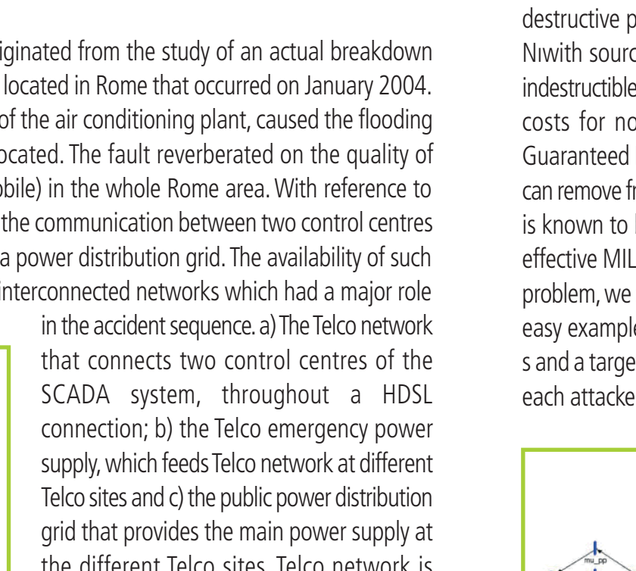
All the algorithms are based on the BDD representation of the connectivity function.

BDD Representation of Network Reliability

A BDD represents a Boolean expression by means of the Shannon's decomposition principle.
The reliability can be computed on the BDD using the following recursive formula:

$$F = x_1 \wedge F_{x1=1} \vee \overline{x}_1 \wedge F_{x1=0}$$

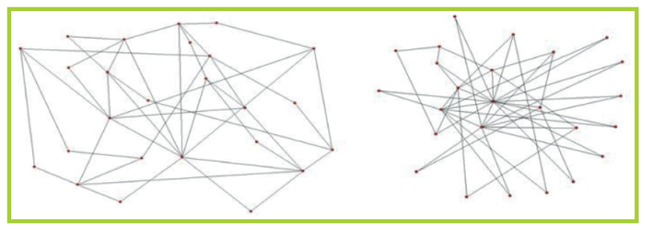
$$P\{F\} = p_1 P\{F_{x_1=1}\} + (1-p_1) P\{F_{x_1=0}\}$$
$$= P\{F_{x_1=0}\} + p_1 (P\{F_{x_1=1}\} - P\{F_{x_1=0}\})$$



The figures reports a regular network with 5 nodes and the corresponding BDD

Reliability as a Function of the Network Structure

One relevant property of networks is that the connection between any two nodes can be usually achieved through a number of redundant paths, thus making the connection intrinsically reliable. Two topological classes are relevant for representing Critical Infrastructures: Random Graph (RG) and Scale Free (SF) networks.



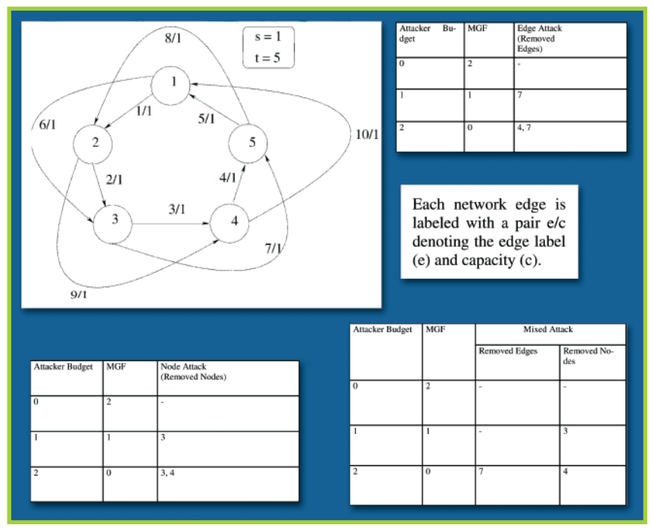
A Random Graph and a Scale Free networks

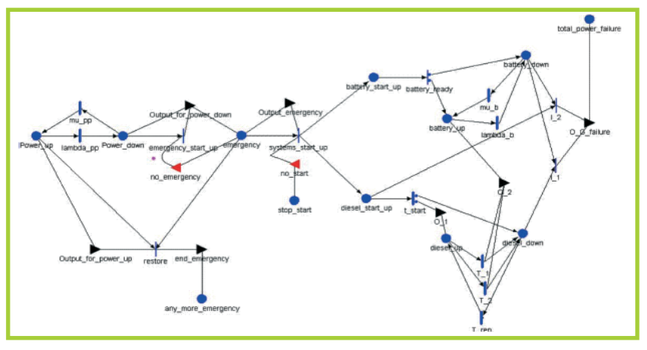
		Random Networks			Scale Free Networks		
#nodes	#edges	#minpaths	# BDD nodes	(s,t) reliability	#minpath	# BDD nodes	(s,t) reliability
20	72	2046	10032	0,98885	263	266	0,98010
25	92	21040	32653	0,98886	2651	5019	0,97815
30	112	119033	708801	0,98906	4704	23978	0,98001
40	152	6757683	n.a	n.a.	73680	n.a	n.a.
50	192	n.a	n.a	n.a	n.a	n.a	n.a

NRA results from RG and SF networks of different size

MGF: A tool for computing the Maximum Guaranteed Flowin Communication Networks

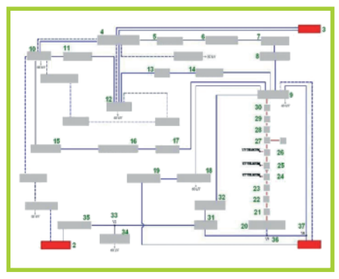
Given a communication network, we address the problem of computing a lower bound to the transmission rate between two network nodes notwithstanding the presence of a malicious attacker with a given destructive power. Formally, we are given: a link capacitated network Niwith source node s and destination node t, a budget B, a set Q of indestructible nodes of N, a set W of indestructible edges of N, destruction costs for nodes and edges. We want to compute the Maximum Guaranteed Flow (MGF) from s to t when an attacker with budget B can remove from N nodes not in Q as well as edges not in W. This problem is known to be NP-complete for general networks. Still, resting on an effective MILP (Mixed Integer Linear Programming) formulation of the problem, we can solve instances with thousands of nodes. The following easy example shows the tool input (i.e. a network with a source node s and a target node t) and possible tool outputs (i.e. tables showing, for each attacker budget, the MGF along with possible attacks).





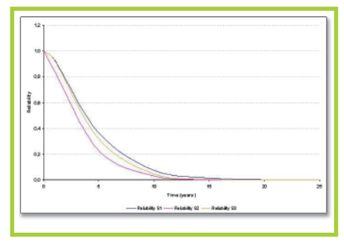
SAN model of Telco emergency power supply

On the loss of main power, Telco emergency power supply is demanded to start. The main power supply may be recovered at any time and the emergency supply is stopped. Batteries are first started with a certain probability and may fail or become exhausted. Diesel generators, after a successful starting, do not provide power instantaneously. Diesel failure may occur in two modes: Failure to start or failure to run. The complex operation of Telco emergency supply is modelled by means of a SAN model, shown in figure.



Reliability Computation of the power distribution grid

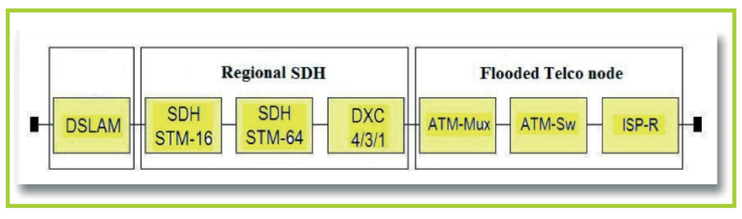
The Figure shows a portion of a regional power distribution grid. Large rectangles represent primary substations small rectangles secondary substations. Nodes, 1, 2, 3, represent the substations of the national power transmission grid. The secondary substations named 24, 25 and 26 provide main power to a Telco node.

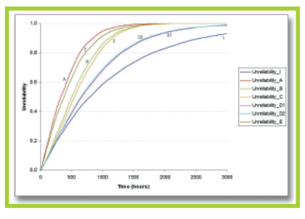


The Reliability of connection from source nodes 1, 2, 3 to node, 25 has been computed using the NRA tool

Reliability Block Diagrams (RDB) model of Telco network

We assume that any failure of a constituent element/ segment of Telco network will not affect the failure of other network element/ segment. Then we resort to RBD, a combinatorial method, implemented through a well known commercial tool ITEM software. Each block is composed by a hierarchy of series/ parallel of RBD sub models, till the basic components (of known failure/repair).





Autori: A. Bobbio[1], R. Terruggia[1], E. Tronci[2], E. Ciancamerla[3], S. Di Blasi[3], M. Minichino[3]
[1]Università del Piemonte Orientale, [2]Università di Roma La Sapienza, [3]ENEA
www.cresco.enea.it