# High-level modelling of critical infrastructures' interdependencies

Simon Delamare*, Alpha-Amadou Diallo and Claude Chaudet

GET/ENST – LTCI UMR 5141
46 rue Barrault
75013 Paris, France
E-mail: simon.delamare@enst.fr
E-mail: Alpha.Diallo@enst.fr
E-mail: Claude.Chaudet@enst.fr
*Corresponding author

**Abstract:** Due to the increasing demand in services' quality and the growing concerns about external threats, the protection of critical infrastructures has recently become a major concern. In this article, we study the potential effect of interdependencies that may occur between two of these infrastructures: the telecommunication networks and the electrical network. In the absence of side protection mechanisms such as multihoming or batteries, these types of networks highly depend on each other. A failure of some component in one of these architectures may cause a fault in the other, for example, when an electrical outage occurs, routers may be switched off as soon as their battery has depleted.

This can lead to cross-domain cascading effects in failures propagation that cause general service unavailabilty. To understand this phenomena, we propose a model that describes the behaviour of these interdependent systems. We show on realistic topologies that simple failures can lead to failures propagation and we derive the potential risk scenarios.

**Keywords:** critical infrastructures; modelling; system interdependencies; electrical network; telecommunication network.

**Reference** to this paper should be made as follows: Delamare, S., Diallo, A-A. and Chaudet, C. (2009) 'High-level modelling of critical infrastructures' interdependencies', *Int. J. Critical Infrastructures*, Vol. 5, Nos. 1/2, pp.100–119.

**Biographical notes:** Simon Delamare obtained an MSc in Computer Networks at Université Pierre et Marie Curie, Paris 6, France, in 2006. He is currently working towards a PhD at TELECOM ParisTech (ENST). His interests include end user services availibilty, overlay networks and routing protocols in IP networks.

Alpha-Amadou Diallo obtained his MSc in Computer Networks at the University of Paris 6, France, in 2006. He is currently a PhD student at TELECOM ParisTech (ENST). His interests are in reliability and the topology design of computer networks. He is also interested in critical infrastructures protection and networks interdependencies phenomena.

Claude Chaudet is an Associate Professor in the Computer Science and Networking Department of ENST (TELECOM ParisTech) one of the top-ranked French engineering schools. He received his PhD in 2004 and has been part of the department since 2005, teaching and performing research in networking. His research interests include understanding and proposing solutions for the security of critical infrastructures. He has been part of the Integrated Risk Reduction of Information-based Infrastructure Systems (IRRIIS) project (ICT-FP6 trust and security programme) since 2006, which aims to characterise and solve the interdependencies problems that may arise between telecommunication and power networks.

This work has been partially funded by the EU projects IRRIIS and Dependability and Security by Enhanced Reconfigurability (DESEREC) under the IST programme of the Sixth Framework Programme (FP6-2005-IST-4).

## 1 Introduction

As humanity evolves, people become more and more dependent on technological facilities. Electricity, and energy in general, has become a primary need in our societies. Telecommunication networks, in the general sense, are also taking on more and more importance in everyday life. All the infrastructures allowing the distribution of energy, information, water, *etc.*, present common characteristics. First of all, they are usually composed of many kinds of equipment, somehow forming a network. Secondly, their destruction could have a great impact on the well-being of modern societies, sociologically or economically.

Great efforts have been deployed these past few years to enhance their individual robustness and most of them are nowadays relatively robust. However, due to the interdependencies existing between these infrastructures, the strategy which consists of ensuring the protection of a single technology is not sufficient. For instance, electrical and telecommunication networks are more and more dependent on each other. Monitoring of the electrical infrastructure components pass by one or several telecommunication networks that require power to operate normally.

These interdependencies are natural, but have the effect of accentuating cascading effects and making these critical infrastructures more vulnerable to intelligent attacks. It is possible today to attack an electrical network by artificially triggering emergency response mechanisms using the telecommunication network. There is therefore a great need for characterising these phenomena and finding appropriate and generic solutions.

This article presents a study on the interdependencies between telecommunication and electrical networks. The only purpose of telecommunication networks is to make information exchanges between distant users as convenient and efficient as possible. To reach this goal, a set of equipment, routers and high-speed links, if we consider the core network, deliver the information from its emitter to its receiver. Several types of networks exist, fixed or mobile, wired or wireless, which are interconnected together and form a global network. These heterogeneous networks carry various types of information, like web pages, audio or video. We will limit our study to the case of a static wired network dedicated to the management of an electrical power grid.

Our purpose is to evaluate the importance of the reactivity of the telecommunication network, which is usually able to self-reconfigure on the propagation of failures in an electrical network. We think that some problems require a global view of the state of the electrical network in order to be appropriately solved. Therefore, maintaining connectivity between the control centre of the electrical infrastructure and any failed component seems an important goal, which we will try to characterise in detail hereafter. This work intends to lay the first stone in the construction of an interdependencies-related problem scenario basis that may be used afterwards to design and evaluate critical infrastructures.

Section 2 reviews some mechanisms defining the performance of both types of networks as well as the common techniques that have been used in each infrastructure modelling, independently or conjointly. We then present and explain the choices we made for simulating both infrastructures in Section 3. The simulation results are discussed in Section 4.

## 2 Related works

The fields of modelling and simulation of telecommunication and electrical networks have generated much contribution since computers have become powerful enough to represent and simulate the behaviour of these complex systems. This section reviews classical strategies and objectives of the simulation of both types of infrastructures and is concluded by a sketch of the state of the art in joint simulation of electrical and telecommunication infrastructures.

### *2.1 Telecommunication networks*

Failures in telecommunication networks can have several causes, as described in Vasseur *et al.* (2004). Some of them are inherent to the telecommunication network itself, for instance when a cable is cut or when a router's software fails. These failures, which happen randomly, are usually caused by human mistakes or by the natural wear of physical components. They are often initially limited to a single equipment, even though their effect can easily propagate among the whole infrastructure with more or less severity. Some failures may, however, result from a conscious will to harm the network, for instance denial of service attacks (Garber, 2000) performed against a service provider. These malicious attacks may be composed of several coordinated and intelligent actions, which makes them harder to detect in time and thus to prevent. Finally, failures may be caused by interdependencies between infrastructures, as studied hereafter. From a given service provider's point of view, all these causes have similar effects: the unavailability of the service for a given period of time.

When it comes to the widely used service of allowing communication between distant endpoints, telecommunication networks were conceived with a certain amount of redundancy in mind. This allows them to recover from the loss of a certain number of equipment in a reasonable amount of time. There are obviously unrecoverable failures, at least in an automatic manner. For instance, when a large part of the infrastructure is destroyed, physically separating peers, no software technique will be able to detect a path that does not exist anymore. However, as long as the physical-level connectivity is preserved, a set of mechanisms, namely routing, shall be able to restore communication capabilities above the cyber layer in a bounded time.

The problem we are interested in here concerns the routing capability of the telecommunication network, in other words its capacity to provide a functioning communication path. In internet-like networks, each router in the infrastructure has to know, for every destination, the next router on the route which it will send the messages to. Depending mainly on the size of the considered infrastructure, the routing mechanism can be configured manually, once and for all, or can be automatically set up and dynamically updated when a failure occurs. When the time to recover from a failure becomes a key issue, for instance when other critical infrastructures depend on the existence of this route, the use of a fast and dynamic routing system seems necessary.

In Internet Protocol (IP) telecommunication networks, which are the networks we consider in this article, the actors performing this maintenance are called routing protocols. They can be classified into several categories. Some protocols are dedicated to the routing *between* networks belonging to different operators, also called Autonomous Systems (ASs). In this category, the Border Gateway Protocol (BGP) (Rekhter and Li, 1994) is the most common mechanism. Others protocols, the ones we will be interested in later on, are dedicated to allow routing *within* an AS. These protocols' principles may differ from BGP's behaviour or not. Each AS administrator is able to use the strategy that best fits its needs. Static routing is sometimes used in small-scale infrastructures but becomes inconvenient in ASs composed of several dozens of routers due to the human maintenance cost they generate.

Among the dynamic intra-AS routing strategies, two main categories exist. Distance Vector (DV) protocols, like RIP (Malkin, 1998) or IGRP (Cisco, 1991), only require communication between neighbours' nodes. In these schemes, each router sends to all its directly connected peers the set of the lengths of the shortest paths it knows towards each destination in the network. Upon reception of such a message, a router is able to compare the announcements from all its neighbours and select among them the best next hop for each destination. Another strategy, called Link State Routing (LSR), relies on the regular diffusion of the whole local topology in messages called LS_Update, obtained by periodically probing every connected neighbour. Every node regularly broadcasts this information to every other node in the network or when some particular events occur. Each node therefore knows precisely the whole topology and is able to compute the shortest paths locally using Dijkstra's algorithm (Dijkstra, 1959). OSPF (Moy, 1998) and IS-IS (Oran, 1990) are the most widely deployed representatives of this category.

In LSR schemes, when a router or a link fails, its neighbours will sooner or later detect it and send a modified LS_Update message to all other routers, containing the failure notification. Upon reception of such a message, every router executes the shortest path algorithm, computing new tables that will bypass the failure if possible. The LSR protocols' recovery performance (*i.e.*, the time needed to restore connectivity after a failure) has been studied in previous papers such as Shaikh and Greenberg (2001), Pasqualini *et al.* (2004) and Shaikh *et al.* (2002). These previous works showed that the time necessary to recover from a failure is about several tens of seconds.

Alaettinoglu *et al.* (2000) and Goyal *et al.* (2003) state that one of the main causes for these long delays lies in the failures detection step, which usually requires periodical probing of peers. The failure to respond to a few probes indicates the disappearance of the tested node or of the link between both routers. If this step takes too much time, the immediate solution that comes to mind consists in reducing the probing interval. However, the impact on the network in terms of bandwidth utilisation should be carefully studied, as well as the probability to react to false positives, for instance transient failures.

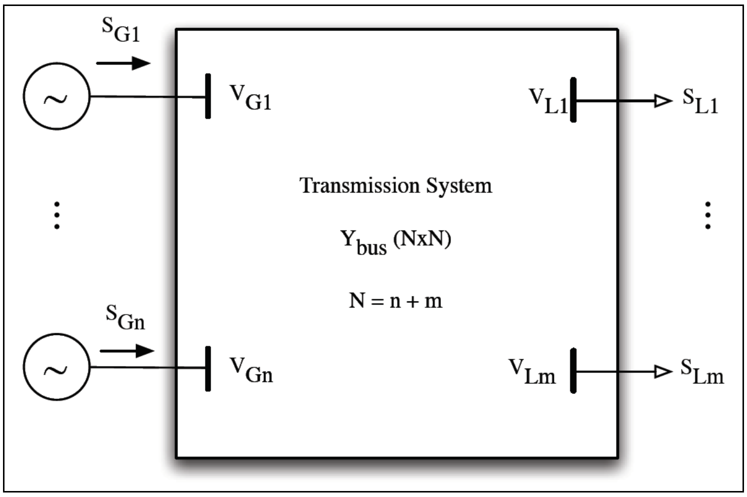
## 2.2 Electrical networks

The modelling of the electrical networks and the effects of cascading failure have captured the interests of many researchers who devoted several works to this topic. There are various procedures[1] to model and simulate these networks. Usually, an electrical system is represented as a set of generators, loads and intermediate nodes (transformers, relays, *etc.*). This representation may be fully represented by an admittance matrix, characterising the whole network. An example of such a matrix is represented in Figure 1. This modelling uses the following fundamental relation to determine the values of the currents and the voltages of each bus of the system:

$$I = Y_{bus} \cdot V,$$

where $I$ is the current, $Y_{bus}$ is the admittance of the bus concerned and $V$ is the effective voltage.

**Figure 1** Typical utilisation of admittance matrix in an electrical network



Unlike telecommunication networks, electrical grid components are highly dependent on each other. The occurrence of a single failure often propagates among the infrastructure, playing an important role in blackouts, which affect these networks. Such propagation may be caused by human actions or inaction or by the misconfiguration of protection systems of the network, which, while trying to insulate the breakdown, can sometimes support its expansion. Dobson *et al.* (2004) carried out studies on such phenomena using three models: the CASCADE model, the branching process and the OPA model.

The CASCADE model is used to determine the number of failed components following a failure propagation. The idea consists in calculating the load factor of a line $J$ of the network:

$$l_j = \frac{L_j - L_{min}}{L_{max} - L_{min}},$$

where $L_j$ is the real load of the line, and $L_{min}$ and $L_{max}$ are respectively the minimal and maximum load of the line. The breakdown of a line causes a load increase $P$ $\left(p = \frac{P}{L_{max} - L_{min}}\right)$ on the other lines. It is then possible to perform a test to know if the load of all the lines is higher than the critical load, corresponding to the case $l_j = 1$. When the load reaches this threshold, the line is cut and the additional load is again distributed among the remaining lines.

The branching process is a transitory Markov process in discrete time used to determine the quantity of energy lost due to a cascading effect. This process considers that the breakdown of the elements at each step independently causes other failures at the following step, with a probability that is exponentially distributed with average $\lambda$.

Finally, the OPA model is close to the software currently used for the electrical networks simulation. Simulation begins with the data of a system in a stable state. At the beginning of the simulation, a randomly selected line is cut, the load is then redistributed on the other lines and, if a line is overloaded, it is cut with a fixed probability at the next step. This iterative process continues until no line is overloaded anymore. For each iteration a calculation is carried out for the whole set of elements until the convergence of the network.

When studying the recent blackouts (*e.g.*, 14 August 2003 in USA, 28 September 2003 in Italy) one can notice that they present similar temporal characteristics. At the beginning successive failures of the lines occur at large time intervals. After a few failures, frequent bursts of failures begin to appear. This phenomenon can be explained by the expansion of a failure. At first, the impacted lines are quite isolated; as time passes, more and more lines are impacted, the failure sooner or later reaching highly connected equipment. Such a failure propagates first to the close nodes and takes more time to reach farther nodes. The distance from the initial point of failure is a factor that influences the faults propagation process because the amplitudes of the oscillations of the electrical network components weaken as they move away from the point of failure.

## 2.3 *Infrastructures interdependencies*

Several research projects and programmes are interested in the cascading effects of failures resulting from the interdependencies that may exist between critical infrastructures. For example, the Joined Infrastructure Interdependencies Research Program (JIIRP) project in Canada works to promote this research sector and to federate both public and private actors working in this field. The Critical Infrastructure Program Protection (CIPP) project in the USA seeks to integrate disciplines, policies and technologies to improve the safety of cyber-networks, the physical systems and the economic processes of the national critical infrastructures. The Integrated Risk Reduction of Information-based Infrastructure Systems (IRRIIS) project in Europe aims to develop tools for interdependencies simulation and information exchange between operators of electrical and telecommunication networks.

Several contributions also propose modelling and simulation results on the critical infrastructures interdependencies phenomenon. For example, researchers of North Carolina University published a simulation model based on the multi-agents approach (Tolone *et al.*, 2004). This model is based on an architecture with agents deployed on several infrastructures components. These agents supervise the installations and communicate to exchange status information. This information can include the description of changes that occurred within an infrastructure and the causes of these changes can be obtained, thanks to a knowledge base filled beforehand. Some works provide communication facilities between several simulation software, leading to modelling and synchronised simulations in order to study, through various scenarios, the interdependencies between these infrastructures. The High Level Architecture (HLA) project of Tucci and Revertiria (2001) is a typical example of this kind of software. The major difficulty in the conception of such systems lies in the fundamental differences existing between discrete events simulators, used for instance in the telecommunication networking field, and continuous time simulators, used for instance in electrical networks dimensioning.

IEEE researchers have also developed a tool for electrical networks simulation, taking into account information coming from a communication network. The Electric Power and Communication syncHronizing Simulator (EPOCHS) (Hopkinson *et al.*, 2006) basically consists of a communication interface between the electric simulators PSCAD/EMTDC and PSLF and the telecommunication network simulator NS-2. This interface of communication allows the simulators to exchange information, keep synchronised and to observe the operation of the electrical supply network while varying various parameters of the communication network (the packets loss rate, for example).

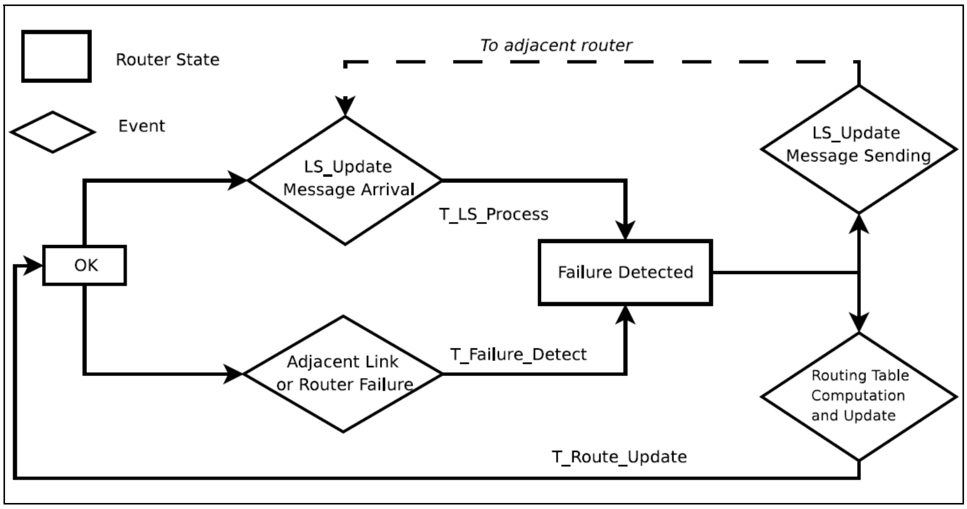
## 3 Architectures modelling

### *3.1 Telecommunication network modelling*

Concerning the modelling of the telecommunication network, several levels of granularity may be applied. Usually, simulations of telecommunication networks are performed using a very fine grain, considering every packet or even every bit transmitted. This type of simulation is usually very useful when investigating the behaviour of a protocol or to evaluate an architecture. On the opposite side, a telecommunication network may be represented as a classical graph and all graph theory algorithm (max flow, weighted shortest-paths, *etc.*) may be applied. This second type of modelling is often useful to determine some pure topological results.

In this study we are interested neither in very coarse simulation, nor in detailed results. The modelling we chose for the telecommunication network elements is represented in Figure 2. We only consider the routing infrastructure and will restrict the analysis to the routing capability of the network. Each router may basically be in two distinct operating states, depending on its perception. Either it seems to be perfectly functioning (OK state) or it has detected a failure (Failure Detected state). Indeed, the OK state represents the situation in which routing tables appear to the router as being in agreement with the network topology and no new node failure has been detected or reported since the last transition to the OK state. The Failure Detected state represents the opposite situation, in which some problem has been identified in the network that has not been solved yet.

**Figure 2** Modelling of a single router's status


Router State
Event
To adjacent router
LS_Update Message Arrival
LS_Update Message Sending
T_LS_Process
OK
Failure Detected
Adjacent Link or Router Failure
T_Failure_Detect
Routing Table Computation and Update
T_Route_Update

A router leaves the OK state when it detects that an adjacent link or router fails. In this case, firing the transition takes a time *T_Failure_Detect*. The second event that may trigger such a transition is the reception of a LS_Update message from one of its neighbours, informing the router that a failure has occurred somewhere in the network. In this case, the router requires a time called *T_LS_Process* to decode and process this message. Once such a failure is detected, the router propagates the LS_Update message to its neighbours and begins to compute a new routing table. This process takes a time *T_Route_Update*, after which it goes back to the OK state.

The modelling of this router's state leads to the calculation of the time required for a router to restore connectivity after a failure, according to the number of hops between the router and the point of failure. $T\_Recovery(N)$ represents the time needed to recover from the failure of a router located at N hops from itself. A distance $N = 0$ represents the situation in which the router is directly connected to the failed link or to the failed router. In this situation, the router needs first to detect the failure and then to update its routing table. Therefore, $T\_Recovery(0) = T\_Failure\_Detect + T\_Route\_Update$. If $N = 1$, the failure has to be detected by the router adjacent to the failure and the LS_Update message has to be sent. Afterwards, any router which receives this message has to process it and update its routing table. In this case, $T\_Recovery(1) = T\_Failure\_Detect + T\_Transmission + T\_LS\_Process + T\_Route\_Update$, where *T_Transmission* is the time needed to transmit the LS_Update message to the adjacent router. In the general case, the failure has to be detected, after which the LS_Update messages have to be transmitted and processed by each router between the failure and the destination router, and finally each receiving router has to update its routing table. Therefore, $T\_Recovery(N) = T\_Failure\_Detect + N*(T\_Transmission + T\_LS\_Process) + T\_Route\_Update$.

Obviously, every failure will not affect every communication path between every pair of nodes. If we want to know whether communication between two nodes is possible or not, we have to determine how severely a physical failure affects IP routing. Obviously, at the physical level, a path needs to exist after the failure. At the logical level, each node of the path must be able to reach the destination node. The routing table of every node on a path has to be correct to allow the routing to reach a destination node. We consider that a router's routing table is correct for a particular destination node, if the next hop router which must be used is the next router on the shortest path between the routing table's examinated router and the destination router. So, if after a failure, the next hop to reach a particular destination of a routing table is unchanged, the router is not affected by this failure for this destination. Finally, to calculate if communication between two nodes is affected by a failure, we have to check if at least one node on the shortest path between the considered nodes has to change the next hop in its routing table to reach the destination node.

Algorithm 1 summarises this process. To handle multiple failures, we consider a list of failures present in the network. Then, for each failure in the list, we can check if the current state of the network, compared to its previous state, creates some new disturbance in the communication between nodes.

**Algorithm 1** Telecommunication network simulation

```
Input: $G$ : Initial network's graph, $FL$ : Failure list, $T$ : Current time, $A$ Source router,
$B$ Destination router
Output: YES (A and B are able to communicate at time T) or NO
Path = Shortest path between A and B in G without links and routers affected by the failures of FL;
if Path does not exist then
    Return NO;
else
    for each router X on the Path do
        for each failure F of FL do
            $G_{cur} = G$ without links and routers affected by the failures $P$ and prior to $P$;
            $G_{pred} = G$ without links and routers affected by the failures earlier to $P$;
            if Next_Hop(of X, to B, in G_cur) != Next_Hop(of X, to B, in G_pred) then
                if T_Recovery(Distance(P , X)) + Occuring_Time (P) ¿ T
                then
                    Return NO;
    return YES;
```

## 3.2 Electrical network modelling

The electrical networks consist of transport and distribution levels. The transport system carries and distributes great quantities of energy. It is devoted to energies with high and very high voltages (from 90 kV to 400 kV), whereas the distribution network is used with tension ranging between 220 V and 65 kV in Europe.

The topology of the transport level is, in general, a grid to allow the energy flow to be forwarded by various paths and to provide a sufficient quantity of energy to the end user, even if certain parts of the network break down, thus respecting the N-1 level of reliability.

For this work, we only modelled the transportation level (400 kV grid) because its failure generally causes the greater scale breakdowns. The representation of this grid in terms of graphs is immediate. Vertices represent the generators (power plants) as well as the loads (*e.g.*, cities) and edges represent the interconnection lines.

The network and flow simulation uses the max flow algorithms (Edmunds-Karp max flow algorithm), whose application requires weights on the links. To simulate phenomena such as unballasting in a network, it is also necessary to have flow values of each node when the network is in stable and unstable states. The links capacities of the graph are converted into megawatt (MW) on the basis of 400 kV for the lines with a section of 500 mm$^2$ and a density of current 0.75 A/mm$^2$. Then, we carry out an initial calculation to evaluate the electrical flow arriving at each node (load). With this method it is possible to fix an initial value of the loads for every node and the capacities of the transport lines. In the next step, we study the failure propagation within the electrical network. The power-lines faults can be caused by natural phenomena or by the protection system of the electrical network, which acts to disconnect some lines from the network when an irregular voltage or frequency of the electrical flow is detected. The loads of the disconnected lines are then distributed on the remainder of the network automatically, following the electric laws, or manually. This distribution can cause an increase in the load of the other lines, leading to further potential failures.

This phenomenon is the main cause of the cascading effects. Automatic procedures programmed in the impedance relays react to a variation in the electrical frequency by shutting the lines off to preserve their integrity, provoking overloads of other lines. In the following modelling, we simulate such a cutting of a line and immediately compute the maximum flow values. From the calculated flow, we are able to identify the most overloaded line. We consider that this line should be able to send information to the control centre to trigger centralised calculation, leading to an appropriate response.

The communication line to the control centre should therefore be possible as soon as the failure appears. Therefore, we test whether the IP routing layer is able to provide a route between the control centre, a node chosen at the beginning of the simulation, and the overloaded line endpoints. When this communication is impossible within the appropriate delays, the line is supposed to be cut by the automatic procedure of the relays. We then perform another test to know whether the change of network topology has an influence on the electric sink associated with the link.

Three situations are possible: First, this cut does not affect the sink node. In this case, simulation continues normally. In the second situation, the cut causes a reduction in the flow incoming to the node and a communication is possible between this node and the control centre. In this situation, unballasting operations may be carried out and the situation resolved. Finally, in the case where there is a flow reduction and no communication is possible, the node is considered as failed and the process is iterated.

### *3.3 Interdependencies modelling*

The dependence of telecommunication networks on power, and therefore on the electrical network, is obvious. However, deriving realistic interdependent scenarios solely from this information is a thorough task. Most of the equipment of the communication network are equipped with Uninterruptible Power Supply (UPS) and similar systems to provide energy when electrical network failure occurs. In spite of these systems, some communication network users are sometimes penalised by micro failures. For instance, on 26 March 2006, Redbus, a French provider of managed data servers, suffered a failure due to several micro electrical failures.

### *3.3.1 Telecommunication infrastructure dependency on electrical infrastructure*

Router and network equipment in general need electrical power to work. Therefore there is a clear dependency in this direction. In our modelling, we decided to link every router to an electrical node in order to model this dependency. Depending on the number of electrical and telecommunication nodes, several routers may depend on a single power source. When an electrical node does not receive power anymore, the routers that depend on it immediately stop functioning. We neglected the use of UPS systems in these infrastructures.

### *3.3.2 Electrical infrastructure dependency on telecommunication infrastructure*

In the model we study in this article, we consider that the exploitation, management and monitoring operations originating from the control centre of the electrical network are done *via* a communication network functioning with the usual IP communication protocols. Even if the operators of the electrical networks may use private networks, the appearance of new services relating to these networks, such as automatic clients' consumption logging or control centre access from mobile terminals, can lead to a wide use of the internet in these scenarios.

Topologies, in the general case, may vary greatly. The exact characteristic of the physical interconnection of routers in a telecommunication network, or the sketch of an operator's electrical network are defined by the spanned geography and therefore have few common characteristics. However, some studies seem to indicate in a general case that both types of networks may exhibit a small-world behaviour (Watts and Strogatz, 1998; He *et al.*, 2007). We consider this hypothesis as a base for the random simulations we perform.

When both topologies are identified, we finally need to model the interconnections, or the dependencies, that may exist between both types of networks. We choose to perform a geographic association because we work with a transport electrical level where a node can represent a substation which provides energy to a whole city; thus it is obvious that the stopping of this substation causes the failure of all the routers of this city. To model this geographic association in random networks, we linked together nodes by order of degree. Higher-degree nodes, in both types of networks, probably represent great cities. This model rests on several hypotheses that seem more or less realistic and we intend to further examine the effect of both types of topologies and their relationships in future work.

The general behaviour of the simulations we perform is expressed more formally by Algorithm 2.

**Algorithm 2** Failure propagation simulation

```
Input: G : Initial network's graph, LC : Links capacities, SimTime Simulation time
S = sum of all nodes representing power plants in the graph;
for each nodes in the graph do
    if Node != S then
        Demand[Node] = edmunds_karp_max_flow(G, S, node);
Choose link to cut to simulate an initial failure;
CCP = Choose the control center position;
while Time ¡ SimTime do
    TimeStep = process the simulation time step taking into account the
    failed links number;
    Time = Time + TimeStep;
    OverloadedLink = most overloaded link in the graph;
    CO = the tail of OverloadedLink;
    A = find the router attached to CO;
    if A and CCP are able to communicate at time Time then
        Reconfigure CO's relay;
        mark OverloadedLink;
    else
        FNode = head of OverloadedLink;
        cut OverloadedLink;
        Flow = edmunds_karp_max_flow(G, S, FNode);
        if Demand[FNode] – Flow ¡ Seuil then
            if FNode and CCP are able to communicate at time Time then
                Demand[FNode] = Flow;
            else
                declare FNode failed;
                isolate FNode;
```

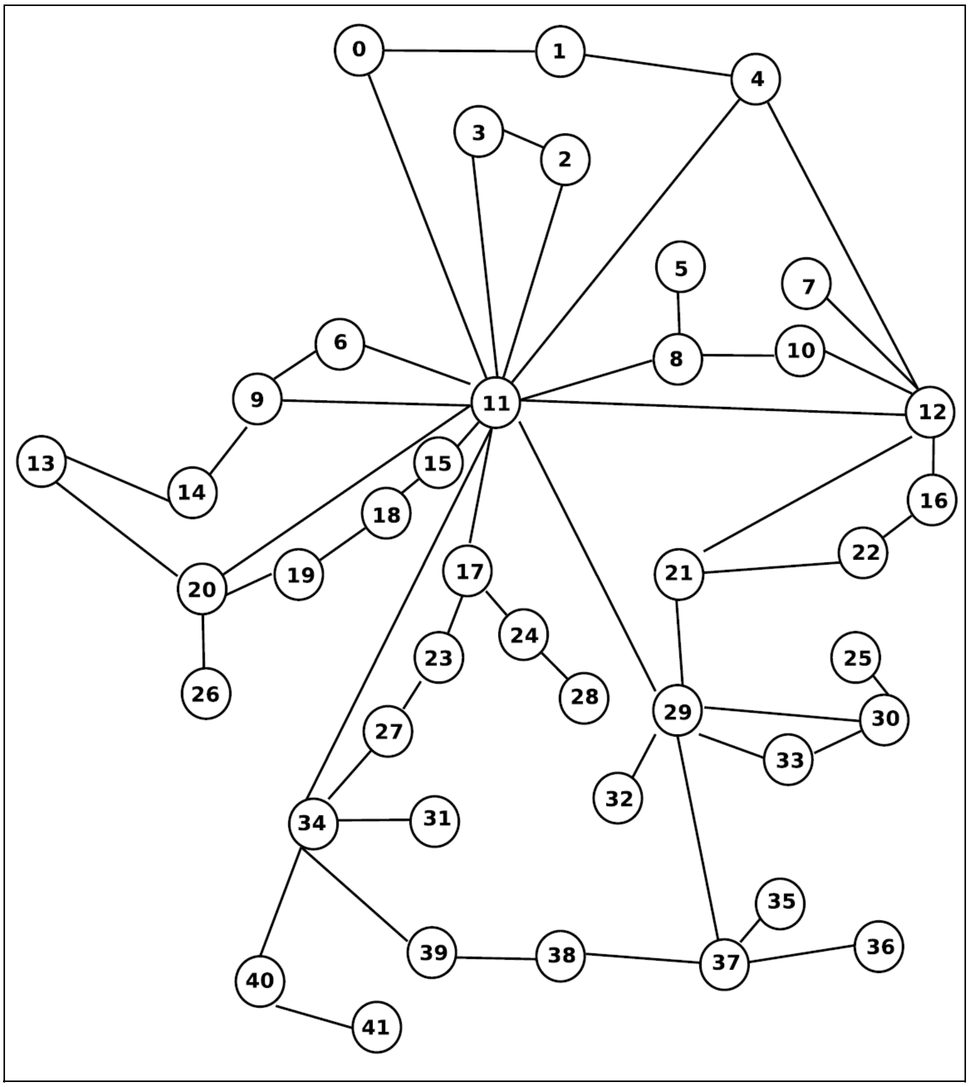
## 4 Experimental results

To demonstrate the relevance of our model and highlight the problems caused by the interdependencies between the electrical and the telecommunication infrastructures, we performed a simulation of our model using real network topologies. In our simulation, we cause the failure of an electrical link and measure its effect. The telecommunication network sometimes fails to provide a communication path that allows the reconfiguration of the electrical infrastructure by the control centre because it is not able to communicate with the electrical nodes to be reconfigured. In this case, the failure may be reconfigured.

### *4.1 Architectures used*

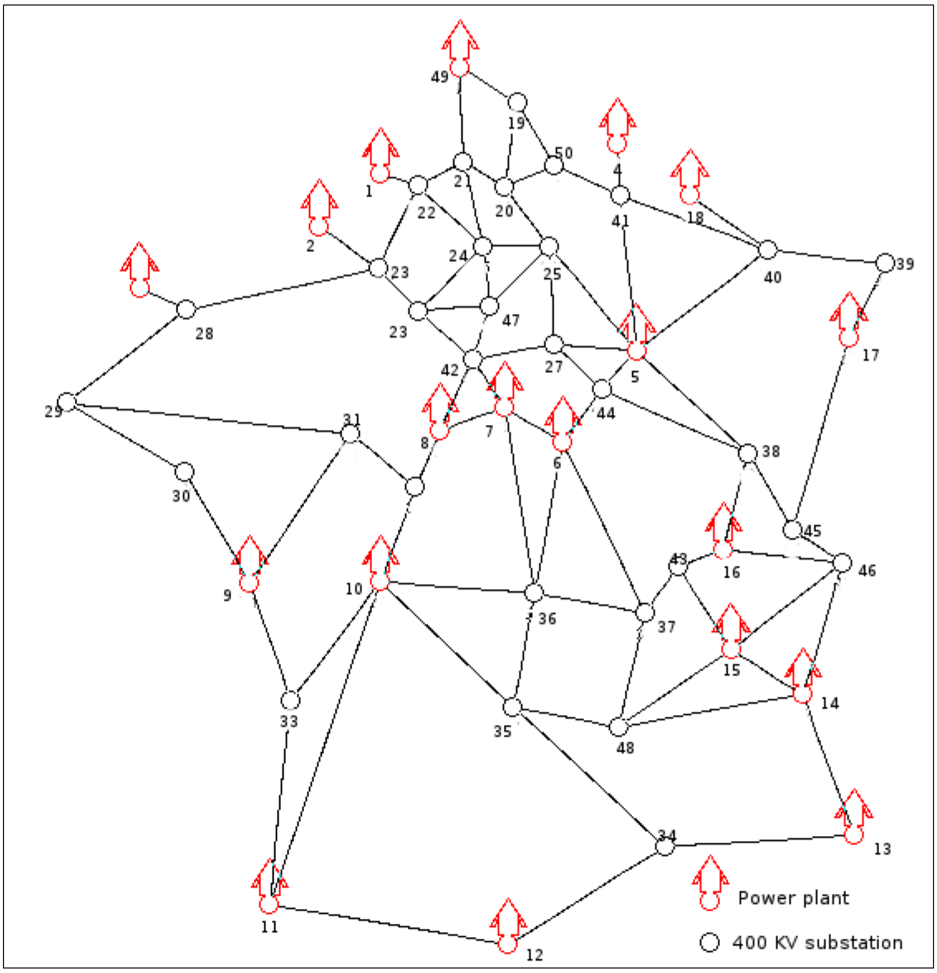
We used the national network of the French internet service provider named Free[2] as our telecommunication network topology. This network is depicted in Figure 3. We used the high-voltage transport network of EDF, the French electrical supplier, as the electrical network. This network is represented in Figure 4.

**Figure 3** The telecommunication network topology



Interdependencies between both networks are set up according to geographical considerations. Routers are empowered by the closest electrical node and an electrical node utilises the closest router to communicate with the control centre, located in Paris.

**Figure 4** The electrical network topology (see online version for colours)



### 4.2 *Simulation parameters and performance criteria*

We decided to fix the average time between two successive electrical failures to 30 sec. As explained in Section 2, the succession between two consecutive electrical failures depends on the number of failures already experienced in the electrical infrastructure.

Based on previous experiments, we set the routing parameters of the telecommunication network to 1 sec for *T_Transmission* + *T_LS_Process* and 5 sec for *T_Route_Update*. In order to model how the telecommunication network reconfiguration performance impacts on the electrical failures propagation, we investigate four cases:

1 The telecommunication network is not dynamically reconfigured in case of failure. The routing protocol used is static. In this case, T_Failure_Detect is set to infinite.

2 The telecommunication network does not detect a failure automatically and needs human intervention. In this case, T_Failure_Detect is set to 600 sec.

3 The telecommunication network detects a failure slowly. In this case, T_Failure_Detect is set to 60 sec.

4 The telecommunication network detects a failure quickly. In this case, T_Failure_Detect is set to 6 sec.

The other parameters we vary between simulation instances are the location of the control centre, which is the router linked with it, and the original electrical link, which fails. The main performance criteria studied in our simulations are the number of electrical nodes and of links which are broken at the end of a simulation instance. We also studied the number of reconfigurations performed in the electrical infrastructure in order to hold back the failures propagation, as explained in Section 3.

### *4.3 One scenario explained in detail*

In order to understand how failures generate other failures, we studied the Free-EDF scenario in detail. In this scenario, the original electrical failing link is (24; 25) and the control centre is connected to router number 10.

Figure 5 shows the measured performance criteria as a function of time required to reconfigure the telecommunication network. As expected, as the telecommunication network reactivity decreases, the number of failures increases. The number of relay reconfigurations decreases as the infrastructure falls before such operations may happen, which further accelerates the occurrence of new failures. A strong correlation seems to exist between these curves, which indicates that the operations are related.

**Figure 5** Electrical infrastructure behaviour according to telecommunication network reconfiguration time

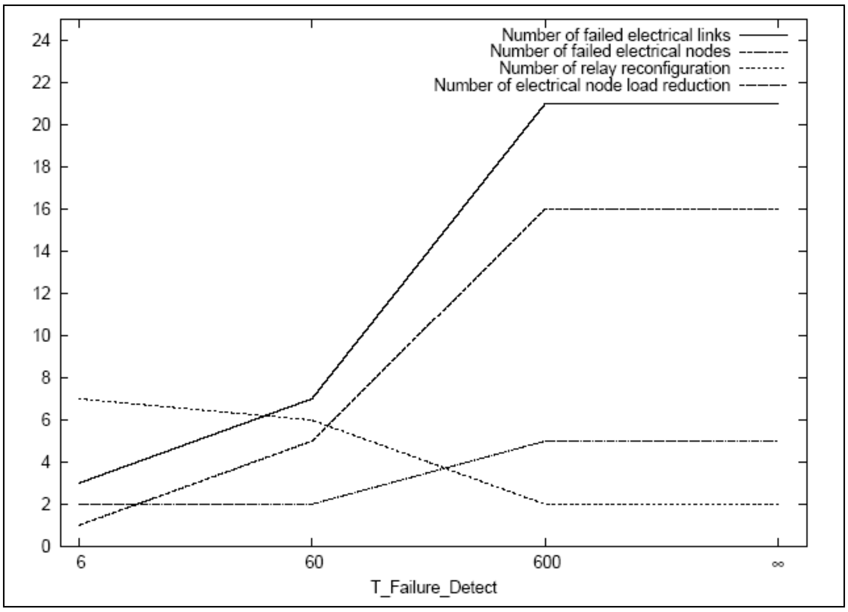


Figure 6 shows the cumulative number of failures during one simulation instance as a function of the simulation time. We can notice that at the beginning of the simulation, failures happen rather slowly. This number reaches a low bound when the telecommunication network is fast enough, but for slower networks, the frequency of link failures increases after some time has elapsed, exhibiting cascading effects. This figure confirms the real behaviour observed in practical scenarios (the Italian blackout, for instance) and shows the importance of a fast-recovering telecommunication network. However, after a certain time, the situation stabilises, which indicates the existence of a natural limitation of failures propagation.

**Figure 6** Failed electrical links apparition according to the simulation processing time

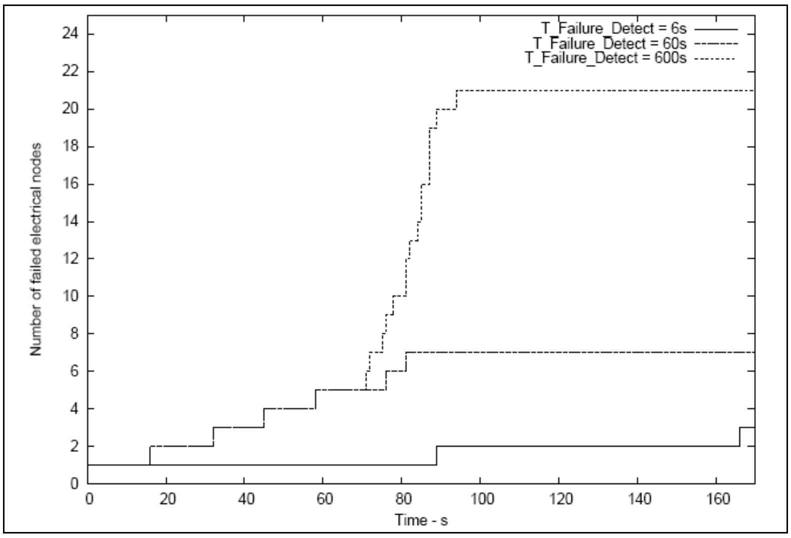


**Figure 7** Electrical infrastructure behaviour according to the ratio between the average electrical failures propagation and the telecommunication network reconfiguration time

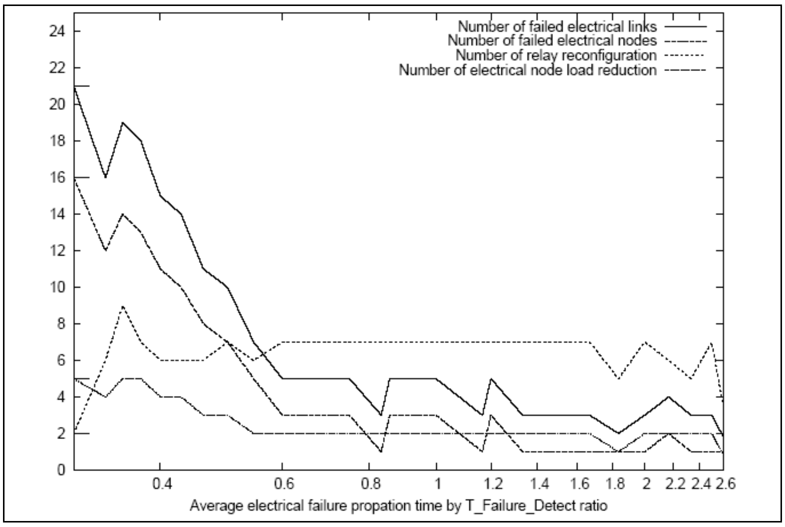


Figure 7 represents the same performance criteria as a function of the ratio between the electrical failures propagation time and the telecommunication network reconfiguration delay. When the telecommunication network reconfiguration time is lower than a certain proportion of the average failure propagation time (value 0.6 in this situation), the number of failures decreases to its lower level, whereas the number of reconfiguration events increases.

These simulations first validate our model, as the results are coherent with our expectancies. The cascading effects appear after a certain time and are severe. The ability of the telecommunication network to quickly reconfigure mitigates these effects.

## *4.4 General results*

The previous scenario was chosen because it highlighted how the telecommunication routing protocol performance could impact on the interdependency problem. But it is one of the worst case scenarios and does not reflect the general behaviour of the system.

We performed a set of simulations based on different scenarios where all of the possible combinations of simulation parameters (the telecommunication network reconfiguration performance, the original failing link and the control centre location) were studied.

Figure 8 shows the different measured criteria of the electrical infrastructure behaviour according to the network reconfiguration time. These graphs are almost flat, indicating that, in the general case, the dependency of the failure propagation effect on the network reconfiguration time is not systematic. Indeed, this delay becomes particularly important when the electrical node to reconfigure suffers from a loss of network connection, which statistically does not happen that often in random scenarios. However, when the situation arises, the consequences are important.

**Figure 8** Average electrical infrastructure behaviour values according to telecommunication network reconfiguration time

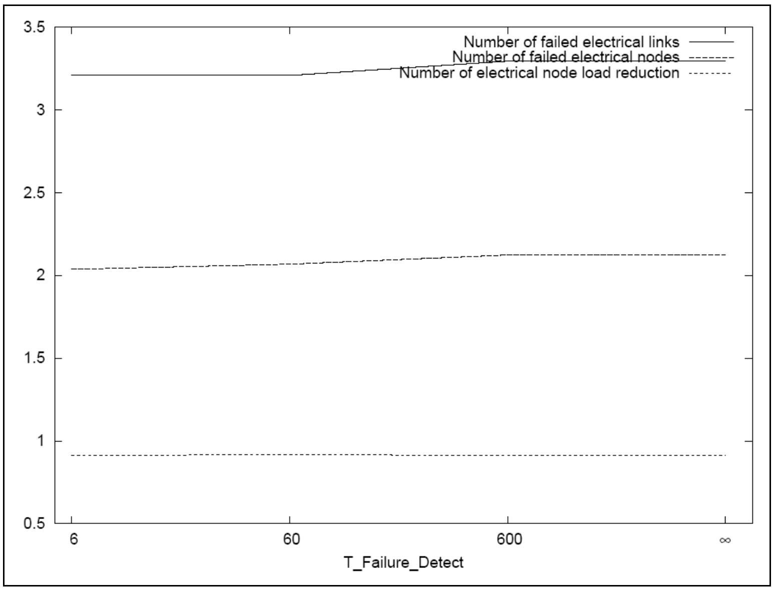
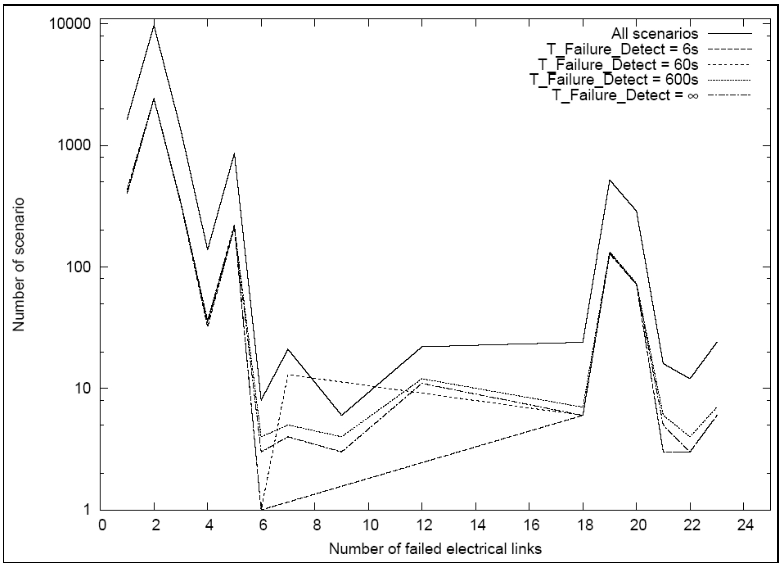


Figure 9 shows, in logarithmic scale, the amount of scenario instances we simulated that resulted in a given number of failures.

**Figure 9** Number of scenarios that resulted in a particular number of failed electrical links



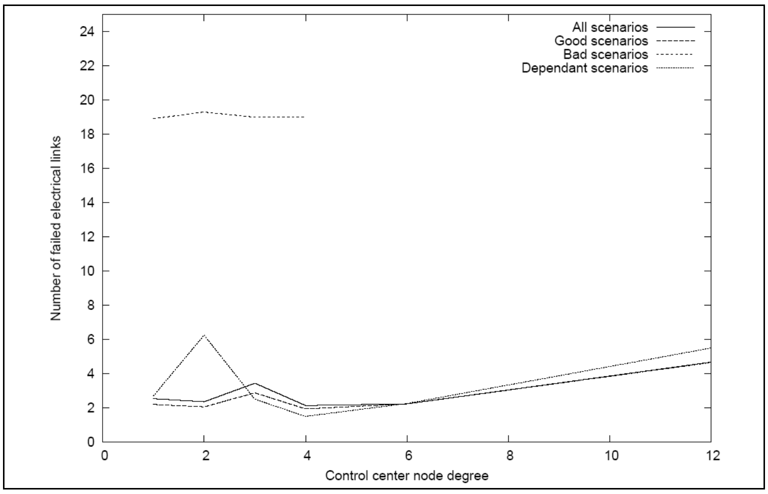
By examining this graph, we can see three separate zones, corresponding to three scenario categories. The first category, called 'Good', regroups the scenarios resulting in a number of failed electrical links lower than or equal to 6, whatever the telecommunication reconfiguration time is. The second category, called 'Bad', includes the scenarios that result in a number of failed electrical links superior or equal to 18, whatever the telecommunication reconfiguration time is. The third and most interesting category, called 'Dependent', comprises all the scenarios in which the number of failed electrical links depends on the telecommunication reconfiguration time. Table 1 shows the number and the percentage of the different scenario cases among our whole set of simulations. It shows that only a few percent of the scenarios are dependent on the telecommunication network reconfiguration time.

**Table 1** Number and percentage of scenarios by category

| *Category* | *Number of scenarios* | *Percentage of scenarios (%)* |
|---|---|---|
| Good | 13 216 | 92.5 |
| Bad | 876 | 6.1 |
| Dependent | 188 | 1.4 |

Finally, Figure 10 shows the average number of failed electrical links as a function of the control centre router's degree. It does not give much information, except that badly behaving scenarios all exhibit a low degree of control centre connectivity. This centre is the keystone of the architecture and should be connected by several redundant paths. Dependent scenarios, in particular, seem to behave badly when the control centre degree falls to a value of 2. In this type of scenario, when a route needs to be recomputed, the resulting route is often much longer. We can see that the absolute number of failure increases with the central node degree, however. In our opinion, this reflects the fact that higher-degree nodes are more likely to be affected by a failure, even though they recover faster.

**Figure 10** Number of failed electrical links according to control centre node's degree



## 5 Conclusion

In this article, we described a modelling of interdependencies between electrical and telecommunication networks, relating the average time between the occurrence of failures in the electrical physical infrastructure and the time required to reconfigure the related telecommunication network.

The results we obtained on a set of simulations performed on a realistic topology as well as on a set of random small-world graphs show that the cascading effects may be limited by the use of a fast-healing telecommunication network, allowing a fast gathering of information at the control centre and enabling taking appropriate actions to reconfigure the electrical network elements.

We studied the parameters that favour or prevent failures propagation and confirmed the intuitive results that a well-connected control centre mitigates the cascading effects. Three types of scenarios seemed to emerge from the general study. Some configurations are less vulnerable to the reconfiguration ability of the telecommunication network, either because the failure has a limited impact, or because it has a great impact, regardless of the communication path's existence. A third category shows a great dependency on the ability of communicating information with the control centre.

Future works include a better characterisation of the three categories of scenarios and a better identification of the relevant graph parameters. More scenarios will have to be evaluated too, especially with different types of random graphs to derive a clear taxonomy of severe failure situations. The results presented here could also be greatly enhanced if the simulation framework we developed could be tested on real topologies.

## References

Alaettinoglu, C., Jacobson, V. and Yu, H. (2000) 'Toward millisecond IGP convergence', Technical Report, October.

Cisco (1991) 'An introduction to IGRP', http://www.cisco.com/application/pdf/paws/26825/5.pdf.

Dijkstra, E.W. (1959) 'A note on two problems in connexion with graphs', *Numerische Mathematik*, Vol. 1, pp.269–271.

Dobson, I., Carreras, B.A., Lynch, V.E. and Newman, D.E. (2004) 'Complex systems analysis of series of blackouts: cascading failure, criticality, and self-organization', *Oak Ridge National Laboratory* Vol. 1, August.

Garber, L. (2000) 'Denial-of-service attacks rip the internet', *Computer*, April, Vol. 33, No. 4, pp.12–17.

Goyal, M., Ramakrishnan, K. and Feng, W. (2003) 'Achieving faster failure detection in OSPF networks', *Proc. IEEE International Conference on Communications*, pp.296–300.

He, Y., Siganos, G., Faloutsos, M. and Krishnamurthy, S.V. (2007) 'A systematic framework for unearthing the missing links: measurements and impact', *USENIX/SIGCOMM NSDI 2007*, April, Cambridge, Massachusetts.

Hopkinson, K., Wang, X., Giovanini, R., Thorp, J., Birman, K. and Coury, D. (2006) 'EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components', *IEEE Transactions on Power Systems*, May, Vol. 21, No. 2, pp.548–558.

Malkin, G. (1998) 'RIP version 2', *Internet Request for Comments RFC 2453*, Internet Engineering Task Force.

Moy, J.T. (1998) 'OSPF Version 2', *Internet Request for Comments RFC 2328*, Internet Engineering Task Force.

Oran, D. (1990) 'OSI IS-IS intra-domain routing protocol', *Internet Request for Comments RFC 1142*, Internet Engineering Task Force, February.

Pasqualini, S., Iselt, A., Kirstadter, A. and Frot, A. (2004) 'MPLS protection switching vs. OSPF rerouting', *Fifth International Workshop on Quality of future Internet Services* (*QofIS'04*), Barcelona, Spain, September.

Rekhter, Y. and Li, T. (1994) 'A Border Gateway Protocol 4 (BGP-4)', *Internet Request for Comments RFC 1654*, Internet Engineering Task Force, July.

Shaikh, A. and Greenberg, A. (2001) 'Experience in black-box OSPF measurement', *Proc. ACM SIGCOMM Internet Measurement Workshop* (*IMW*), November.

Shaikh, A., Isett, C., Greenberg, A., Roughan, M. and Gottlieb, J. (2002) 'A case study of OSPF behavior in a large enterprise network', *ACM Internet Measurement Workshop 2002*.

Tolone, W.J., Wilson, D., Raja, A., Xiang, W., Hao, H., Phelps, S. and Johnson, E.W. (2004) 'Critical infrastructure integration modeling and simulation', *Proceedings of 2nd Symposium in Intelligence and Security Informatics*, Tucson, USA, June.

Tucci, M. and Revetria, R. (2001) 'Different approaches in making simulation languages compliant with HLA specifications', *Proceedings of Summer Computer Simulation Conference*, Orlando, USA.

Vasseur, J.P., Pickavet, M. and Demeester, P. (2004) *Network Recovery*, Chap. 1.2.2, Morgan Kaufmann.

Watts, D.J. and Strogatz, S.H. (1998) 'Collective dynamics of 'small-world' networks', *Nature* Vol. 393, June.

## Notes

[1] http://thunderbox.uwaterloo.ca/_claudio/courses/ece465/ece465 664.html

[2] http://www.free.fr