Rapport Network : La robustesse du réseau électrique européen

Victor Journé, Ludovic Lelievre

I- Introduction

Nos sociétés sont largement construites autour de systèmes de réseaux qui nous fournissent en électricité, en eau, en routes, en télécommunication, etc. Ces infrastructures ont contribué à la hausse de nos conditions de vie et les services qu'ils apportent sont plus ou moins considérés comme acquis. Cependant, des perturbations sur ces réseaux peuvent avoir des conséquences non négligeables sur nos conditions de vie ainsi que provoquer des pertes économiques. Les perturbations sur ces réseaux sont de nature diverses : perturbations climatiques, perturbations techniques, ainsi que le sabotage ou même les attaques terroristes. Ainsi, identifier et éliminer les points faibles de ces réseaux en modifiant leur structure est crucial afin d'éviter de large crise dans nos sociétés.

La robustesse d'un réseau est sa capacité à fonctionner malgré la défaillance d'un nombre fini de nœuds. Plus un réseau est robuste, moins il est vulnérable aux attaques. Les réseaux d'infrastructures modernes sont construits autour d'un nombre important d'interconnexion, ce qui les rend résilients face à des dysfonctionnements aléatoires mais très vulnérables à des attaques ciblées (voir *Attack Vulnerability of Complex Network* – P.Holme et al.). C'est aux conséquences de ces dernières que nous allons nous intéresser. Une attaque est dite ciblée lorsque sont visés en priorité les nœuds les plus importants du réseau, c'est-à-dire ayant un nombre de connexion (degree) le plus élevé.

Le but de notre projet est de comprendre le rôle des réseaux dans l'apparition d'attaques ciblées en cascade dans un système réel, le réseau électrique européen et d'évaluer comment et à quelle coût la structure du réseau pourrait être modifiée de telle sorte qu'il devienne plus robuste face à des attaques ciblées.

La notion de coût est importante à prendre en compte lorsque l'on modifie un réseau existant. En effet, une réponse naïve serait de proposer de relier chaque nœud entre

eux afin de créer un réseau complètement connecté. Il en résulterait un réseau parfaitement robuste mais économiquement inconcevable. L'algorithme proposé par C.M. Schneider et al. dans leur papier *Mitigation of Malicious Attacks on Networks* prend en considération l'aspect économique dans l'amélioration de la structure du réseau : la base du réseau, c'est-à-dire le nombre de nœuds et le nombre de liens, ne doit pas être modifié ; de plus deux liens ne peuvent pas être modifiés si cela augmente la longueur de la connexion. Nous appliquons cet algorithme sur le réseau électrique européen afin d'améliorer sa robustesse.

Dans la partie II, nous caractérisons la structure du réseau électrique européen. Dans la partie III, nous analysons la robustesse du réseau et améliorons sa robustesse à l'aide de simulations.

II- Caractéristiques du réseau électrique européen

A- Les données

Les données sur le réseau électrique européen que nous utilisons dans ce projet est le réseau au sens topologique, et non le réseau de capacité informant de la puissance maximal admissible sur chaque ligne, ainsi que les sites de production. Chaque nœud du réseau correspond à un site de production ou à un générateur, chaque nœud à une ligne de transmission.

L'intérêt principal de ce jeu de données est de fournir la géolocalisation des nœuds du réseau. Cette information nous permet d'une part de représenter le réseau sous la forme d'une carte ; d'autre part, connaissant la localisation des nœuds, nous pouvons calculer la longueur des liens, information que nous utiliserons dans la partie III lors des simulations.

Les données du réseau électrique européen que nous utilisons forme donc un réseau sans direction et sans poids de 1494 nœuds et 2199 liens.

La carte ci-dessous présente les données du réseau électrique européen.

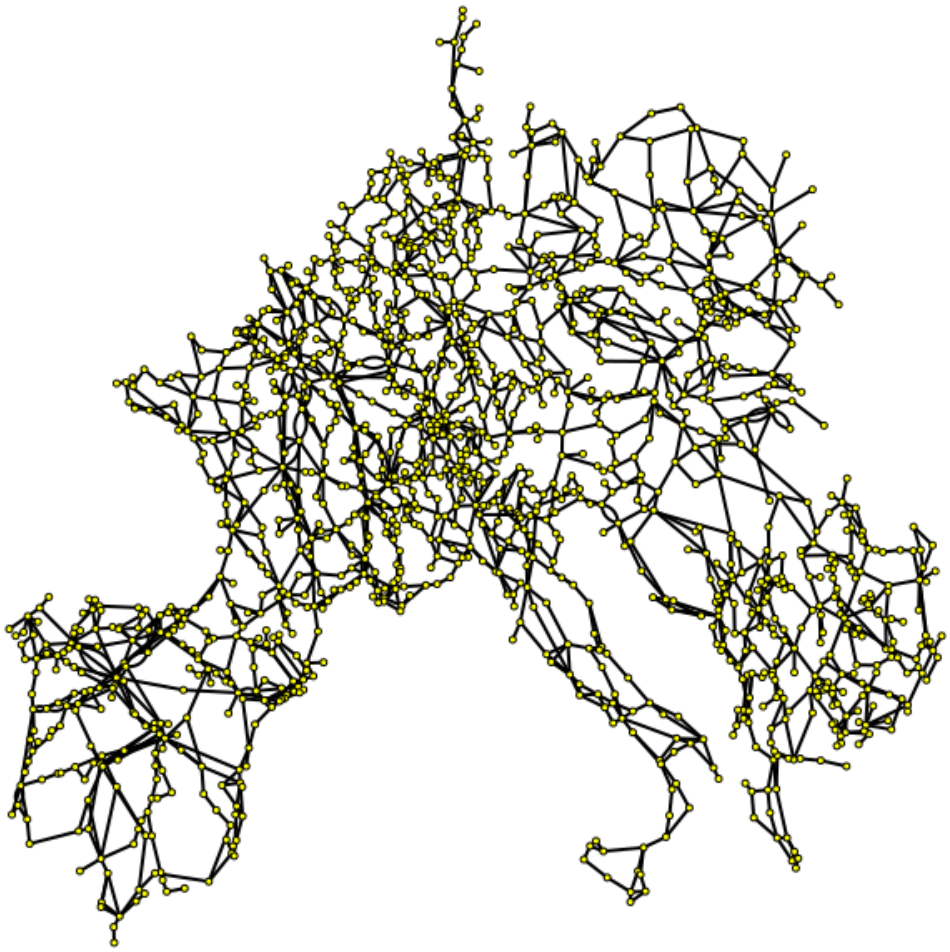

Figure 1 : carte du réseau électrique européen

B- Caractéristiques du réseau

Dans notre analyse de la robustesse du réseau électrique européen, l'importance d'un nœud est définie par son nombre de connexion, c'est-à-dire le nombre de liens qui le relie à d'autres nœuds. La défaillance de ces nœuds aura un très fort impact sur la qualité du réseau. Ce sont donc les nœuds avec une forte connectivité qui seront les premiers attaqués.

Il est donc important au préalable de caractériser la structure du réseau électrique européen en terme de connexions. Pour cela, nous allons utiliser trois statistiques :

- Average degree
- Degree distribution
- Clusters

Average degree :

Le degré moyen d'un réseau exprime le nombre de liens moyens d'un nœud dans le réseau. Plus le degré moyen est élevé, plus les nœuds du réseau sont connectés entre eux. Plus il est faible, plus le réseau est sparse. Le degré moyen du réseau électrique européen est pratiquement égal à 3. Cela signifie qu'un nœud dans ce réseau possède en moyenne trois connexions. Nous sommes donc dans le cas d'un réseau sparse, c'est-à-dire avec beaucoup de nœuds et peu de liens entre les nœuds en moyenne.

Degree distribution :

Le degré moyen d'un réseau, étant par définition une moyenne, ne permet pas d'apprécier l'hétérogénéité des nœuds d'un réseau, c'est-à-dire la répartition de la fréquence des nœuds en fonction de leur degré. Pour avoir une vision plus précise de la connectivité d'un réseau, il faut regarder la distribution des degrés des nœuds du réseau.

L'histogramme ci-dessous (Figure 2) montre que nous sommes en présence d'une distribution homogène, si on ne prend pas en compte les nœuds ayant un degré égale à 1. Cela signifie que la fréquence des nœuds diminue exponentiellement avec son degré. Ainsi un nombre élevé de nœuds a une très faible connectivité et quelques nœuds accaparent un nombre important de connexions. Toutefois, il existe des nœuds avec un degré intermédiaire, ce qui implique que la distribution n'est pas hétérogène. Ceci est une caractéristique importante dans le cas de l'analyse de la robustesse puisque ce sont les nœuds à forte connectivité qui seront supprimés les premiers. Ainsi, comme il existe des nœuds à degré intermédiaire dans le réseau électrique français, il est probable que le réseau résiste mieux à des attaques ciblées qu'un réseau avec une distribution hétérogène.

Clusters :

Le bon fonctionnement d'un réseau est conditionné à la connexion de ses composantes entre eux. La structure du réseau électrique européen est composée d'un cluster. Ainsi, en partant d'un nœud du réseau, il est possible de trouver un chemin reliant ce nœud à tous les autres nœuds du réseau.

Lorsque l'on supprime un nœud du réseau, on supprime également les liens partant de ce nœud. Ainsi lorsque l'on procède à des attaques en cascade des nœuds du réseau électrique, cela a pour effet de diviser le réseau en plusieurs clusters et ainsi d'isoler des segments qui ne sont plus reliés entre eux.

La carte ci-dessous (Figure 3) présente par différentes couleurs les clusters créés après la suppression des 100 nœuds les plus importants du réseau.

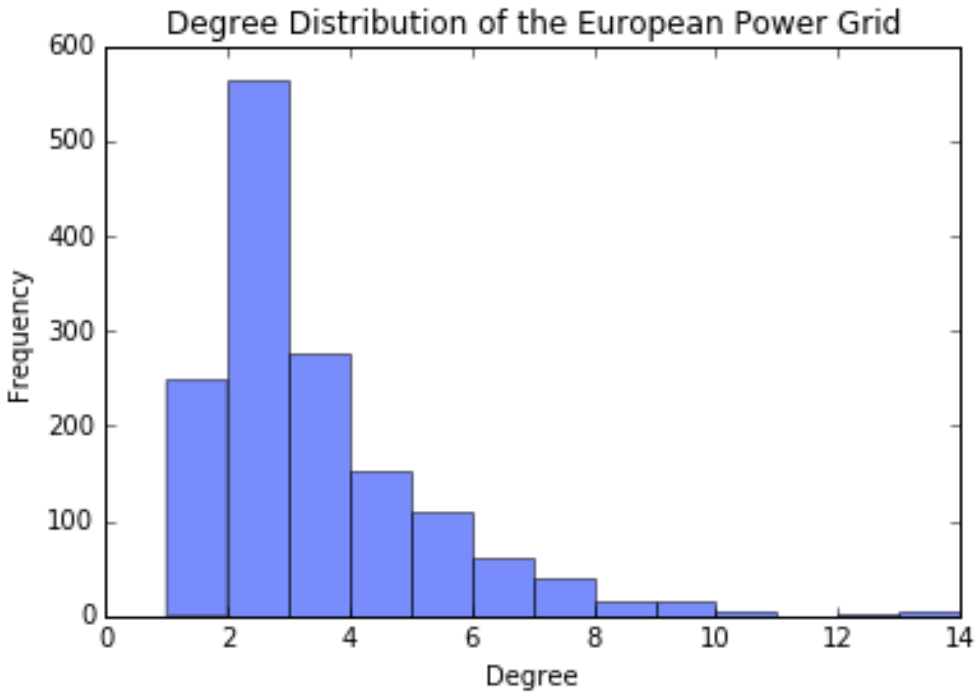

Figure 2 : Distribution du degré des nœuds dans le réseau électrique européen

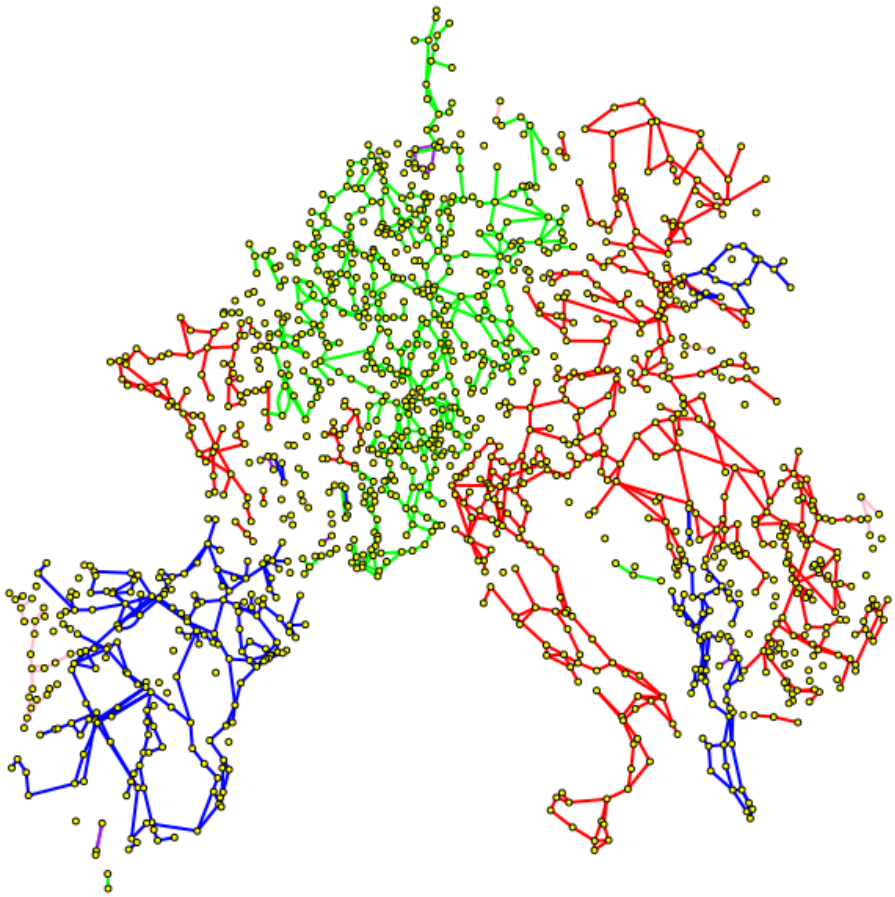

Figure 3 : Formation de clusters dans le réseau électrique européen après suppression des 100 nœuds les plus importants

III- Robustesse

A- Nouvelle mesure de robustesse

Comme seul le réseau au sens topologique est étudié ici, et non pas le réseau de capacité informant de la puissance maximal admissible sur chaque lignes, ainsi que les sites de production et de soutirages, nous faisons l'hypothèse simple que la robustesse caractérise un réseau à ne pas se diviser après des attaques. Cela peut ne pas paraître réaliste au premier abord, car les attaques se focaliseraient probablement d'abord sur les lignes à hautes tensions à forte capacité, ou aux alentours des centrales importantes, mais la capacité du réseau à rester le plus longtemps relié permettrait de résister.

Nous choisissons comme dans le papier *[Mitigation of Malicious Attacks on Networks]* la mesure de robustesse originale suivante :

$$\boldsymbol{R = \frac{1}{N}\sum_{Q=0}^{N} s(Q)}$$

Avec N le nombre de nœud du graphe
Et $s(Q)$ la fraction du nombre de nœuds dans le plus grand sous réseau connecté, après avoir supprimer les Q nœuds de plus haut degré.

Cette mesure de robustesse traduit bien la capacité qu'un réseau fonctionne malgré la défaillance d'un nombre fini de nœuds.

Cette mesure R peut valoir au plus 0.5 pour un réseau entièrement connecté et au moins $\frac{1}{N}$ dans le cas d'un réseau en étoile autour d'un nœud connecté à tous les autres. Dans notre cas R = 0.0694, ce qui est 100 fois plus qu'un réseau en étoile avec le même nombre de nœuds =1494

.

B- Amélioration de la mesure par une procédure d'acceptation/rejet

La mesure de robustesse pour le réseau initial est donc l'aire sous la courbe rouge de la figure suivante (Figure 4). L'aire en verte représente l'amélioration de l'indice de performance grâce à l'algorithme décrit après.

Sous une contrainte de coût, validé si la longueur de ligne à haute tension remplacée est plus courte que dans le réseau initial, il est possible de concevoir un nouveau réseau plus robuste.

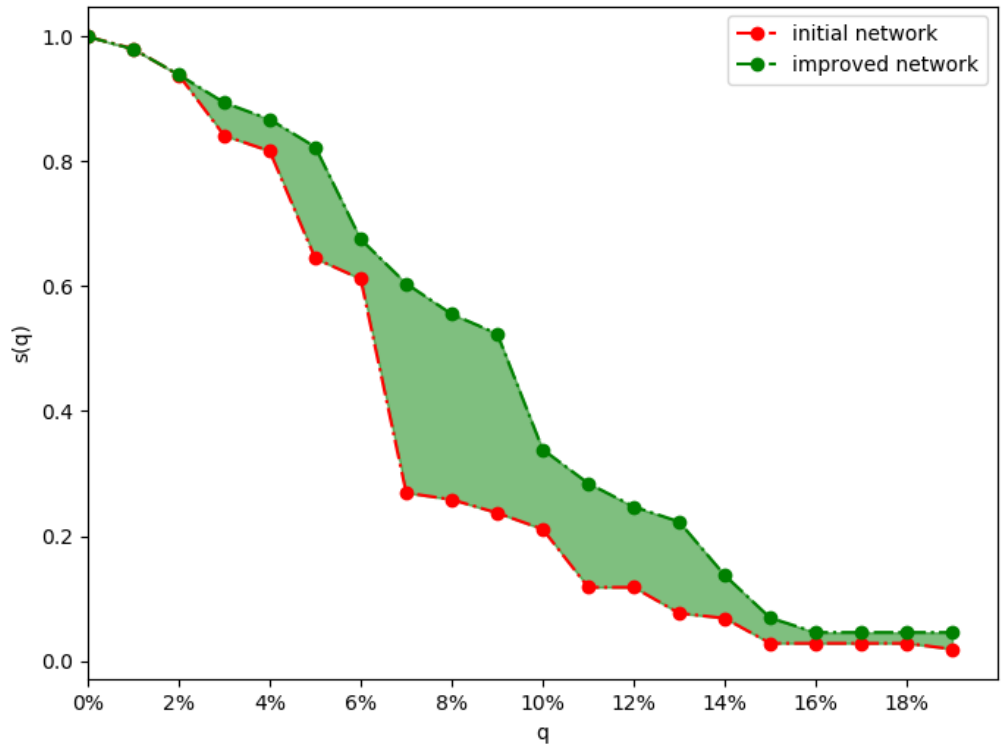

Figure 4 : Mesure de robustesse en fonction du pourcentage q de nœuds détruits

L'algorithme s'inspire de la méthode accept/reject. Il est itératif est requiert de calculer à chaque itération la nouvelle mesure de robustesse. Il faut aussi connaître la longueur de chaque lien pour calculer la fonction de coût associé à la proposition d'échanger deux liens.

Algorithme :

- On tire aléatoirement 2 nœuds i et j et 2 de leurs voisins k et l
- On inverse les liens si les conditions sont remplies :
    1. i,l et k,j ne sont pas reliés (pour ne pas créer une double connexion)
    2. la distance $d(i,l) + d(k,j) < d(i,k) + d(j,l)$. C'est la contrainte de coût)
    3. la robustesse R est améliorée

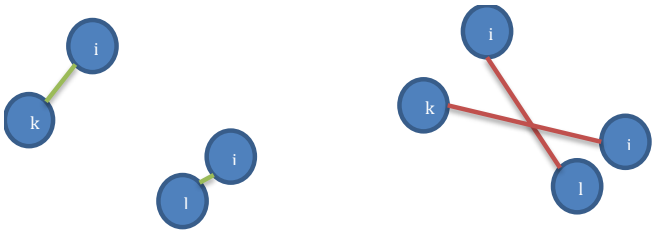

Figure 5 : Illustration de l'algorithme. Les segments rouges remplacent les liens verts sous les trois conditions de l'algorithme

Le remplacement de certains liens est représenté dans la figure ci-dessous. On observe que les remplacements concernent surtout l'Allemagne, la Belgique, l'Espagne du nord ainsi que l'Allemagne et la Pologne.

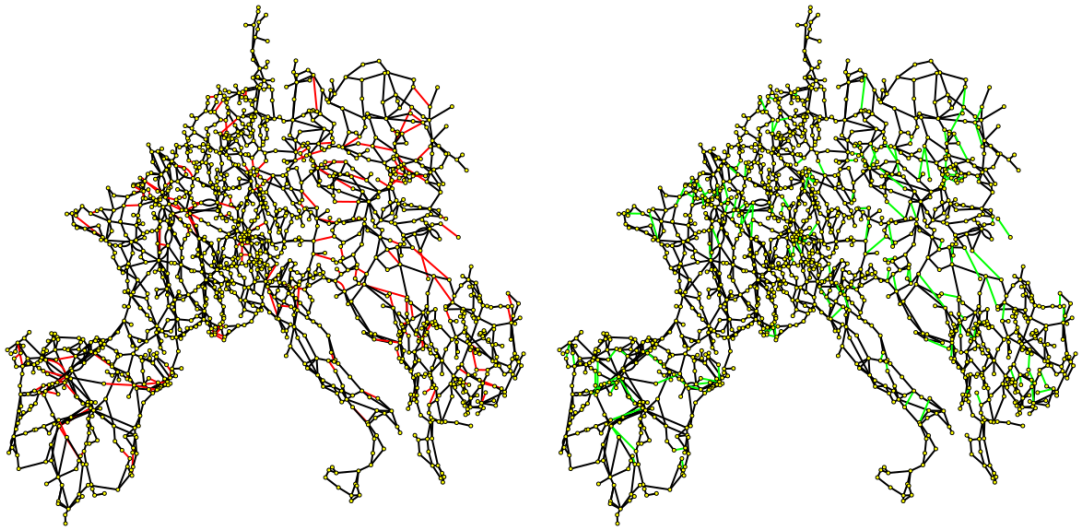

Figure 6 : en vert les liens rajoutés et en rouge les liens supprimés du réseau initial

IV- Conclusion

Dans ce projet, nous avons utilisé une mesure de robustesse qui permet de comparer la robustesse de différents réseaux entre eux. Nous nous sommes servis de cette mesure afin de mener des simulations dans le but d'améliorer la robustesse du réseau électrique européen contre des attaques ciblées à faible coût. L'approche que nous avons utilisée s'est révélée concluante sur un réseau réel, le réseau électrique européen. Nos résultats montrent qu'avec un coût économique raisonnable, la robustesse du réseau électrique européen peut être améliorée de manière significative, tout en conservant le degré de chaque nœuds et la longueur total des câbles du réseau électrique.