C. Alcaraz, E. Etcheves Miciolino, and S. Wolthusen, "Structural Controllability of Networks for Non-Interactive Adversarial Vertex Removal", *8th International Conference on Critical Information Infrastructures Security* vol. 8328, pp. 120-132, 2013.
http://doi.org/http://link.springer.com/chapter/10.1007%2F978-3-319-03964-0_11
NICS Lab. Publications: https://www.nics.uma.es/publications

Structural Controllability of Networks for Non-Interactive Adversarial Vertex Removal

Cristina Alcaraz, Estefanía Etchevés Miciolino and Stephen Wolthusen

October 27, 2015

Abstract

The problem of controllability of networks arises in a number of different domains, including in critical infrastructure systems where control must be maintained continuously. Recent work by Liu *et al*. has renewed interest in the seminal work by Lin on structural controllability, providing a graph-theoretical interpretation. This allows the identification of *driver nodes* capable of forcing the system into a desired state, which implies an obvious target for attackers wishing to disrupt the network control. Several methods for identifying driver nodes exist, but require undesirable computational complexity. In this paper, we therefore investigate the ability to regain or maintain controllability in the presence of adversaries able to remove vertices and implicit edges of the controllability graph. For this we rely on the POWER DOMINATING SET (PDS) formulation for identifying the control structure and study different attack strategies for multiple network models. As the construction of a PDS for a given graph is not unique, we further investigate different strategies for PDS construction, and provide a simulative evaluation.

Keywords: Structural Controllability, Attack Models, Complex Networks

1 Introduction

Controllability theory offers a general, rigorous, and well-understood framework for the design and analysis of not only control systems, but also of networks in which a control relation between vertices is required [1]. The seminal work by Lin [2] provided a graph-theoretical formulation that has only recently become the renewed focus of research [3], which aids in understanding criteria for establishing control over networks. Both the work by Liu *et al*. [3] and subsequent work focuses on the identification of so-called *driver nodes* using non-rigorous maximum matching (to find subset of driver nodes that do not share input vertices) [4, 5]. In this paper, we study an alternative approach based on the POWER DOMINATING SET (PDS) problem, which gives an equivalent formulation for identifying minimum driver node subsets (denoted N_D in the following discussion) sufficient to reach a desired configuration from an arbitrary configuration in a finite number of steps; for a time-dependent linear dynamical system (equation 1):

$$\dot{x}(t) = \mathbf{A}x(t) + \mathbf{B}u(t), \qquad x(t_0) \; = \; x_0 \tag{1}$$

where $x(t)$ is a vector $(x_1(t),\ldots,x_n(t))^T$ representing the current state of a system with n nodes at time t; $\mathbf{A}$ is an adjacency matrix $n \times n$ giving the network topology identifying interaction among nodes, $\mathbf{B}$ an *input* matrix $n \times m$, where $m \leq n$, identifying the set of nodes controlled by a time-dependent *input vector* $u(t) = (u_1(t),\ldots,u_m(t))$ which forces the system to a desired state. The system in eq. 1 is *controllable* if and only if $\text{rank}[\mathbf{B},\mathbf{AB},\mathbf{A}^2\mathbf{B},\ldots,\mathbf{A}^{n-1}\mathbf{B}] = n$ (Kalman's rank criterion). Whilst straightforward, for large

networks the exponential growth of input values as a function of nodes is problematic, giving importance to the work on *structural controllability* by Lin [2].

The robustness of such networks has been studied by Pu *et al*. [5] *inter alia*, while work by both Liu *et al*. [3] and Wang *et al*. [4] has shed light on the effects of attacks (edge and vertex removal) on the network and the subgraph representing the controlling structures, clearly identifying the effect that network topology has on the impact achievable by such removal attacks. One problem immediately arising from vertex removal from a minimal power dominating set is the *reconstruction* and recovery of control.

Direct computation is undesirable as the PDS problem in general graphs has been shown to be $W[2]$-hard by Downey and Fellows [6], also showing that PDS is only $\Theta(\log n)$-approximable for general graphs. However, we argue that sub-optimal approximations are of considerable interest if this allows the efficient re-construction of a power dominance relationship that has only been partially severed.

In this paper we therefore study the effects of different non-interactive attack patterns (i.e. attackers are assumed to choose only a single set of vertices) resulting in vertex and edge removal from control graphs and interactions with the choice of equivalent PDS. For critical infrastructure networks, such as electric power networks or information networks, several topologies are of interest in which the concept of controllability underlines the importance of the technique itself for protection. We therefore study elementary (*Erdős-Renyi*) random graphs, but also small-world (*Watts-Strogatz*) and scale-free (*Barabási-Albert*) graphs, also with preferential attachment and provide simulation results for different parameter sets.

The remainder of this paper is structured as follows: Section 2 briefly reviews related work and the relationship between structural controllability and power dominance while section 3 describes the network models and resulting topologies as well as the derivation of control networks and strategies for attack based on limited vertex removal. We then proceed to study the impact of such attacks on different network and equivalent control topologies simulatively in section 4 before discussing the results and giving our conclusions together with an outlook on our on-going work.

2 Structural Controllability and Power Domination

In eq. 1, the matrix $\mathbf{A}$ gives the network topology, and the matrix $\mathbf{B}$ can be interpreted as the set of nodes with the capacity to drive control. Lin [2] gives the interpretation of $G(\mathbf{A},\mathbf{B}) = (V,E)$ as a digraph where $V = V_{\mathbf{A}} \cup V_{\mathbf{B}}$ the set of vertices and $E = E_{\mathbf{A}} \cup E_{\mathbf{B}}$ the set of edges. In this representation, $V_{\mathbf{B}}$ comprises nodes able to inject control signals into the entire network, i.e. those constituting $u(t)$ in eq. 1.

Two main approaches for determining $V_{\mathbf{B}}$ have been studied; most attention has been paid to the *maximal matching* approach. Liu *et al*. [3] have recently observed that in directed networks, cacti (interconnection point between systems) and matchings in certain bipartite graphs are in a one-to-one correspondence and have gained considerable attention from their study of these structures, using the non-rigorous *cavity method* (applied to solve mean field approaches in statistical physic) for different classes of random directed graphs, notably directed versions of random regular graphs, the Erdős-Renyi random graph, and power-law random graphs. Of particular interest is the identification of minmum subsets of unmatched (*driver*) nodes N_D not sharing input vertices. Matchings in graphs is a well-studied problem, and polynomial algorithms exist [7, 8], but this is not matched by understanding of graphs with fixed degree sequence and is the subject of on-going research that is both of mathematical interest and for motivated by the characteristics of networks as recent work by Pósfai *et al*. shows [9].

The robustness of controllability of several random graph classes including degree sequences found in existing (i.e. complex) networks has been investigated by Wang *et al*. [4], describing a perturbation strategy based on adding edges to graphs, while Pu *et al*. describe the effect of random and targeted vertex removal on matchings in Erdős-Renyi random graphs and scale-free graphs, although we note that the underlying

results have been proven rigorously previously by Bollobás and Riordan [10]. We also note the results by Sudakov and Vu on graph resilience for both local and global properties [11].

In this paper, however, we concentrate on an alternative approach to the study of structural controllability, POWER DOMINATING SET (PDS). This problem was introduced by Haynes *et al*. [12] as a variant of the well-studied problem of domination motivated in part by the structure of electric power networks and the efficient monitoring of such networks. The basic decision problem (DOMINATING SET, DS) is NP-complete with a polynomial-time aproximation factor of $\Theta(\log n)$ as shown by Feige [13]. The PDS problem can be summarised by two rules, simplified by Kneis *et al*. [14] from the original formulation by Haynes *et al*.:

OR1 A vertex in the N_D observes itself and all its neighbours.

OR2 If an observed vertex v of degree $d \geq 2$ is adjacent to $d-1$ observed vertices, the remaining unobserved vertex becomes observed as well.

which is reduced to DOMINATING SET by the omission of **OR2**; whilst we are also interested in the digraph formulation, for an undirected graph $G = (V,E)$ and an integer $k \geq 0$, PDS seeks a set $N_D \subseteq V$ with $|N_D| < k$, which can observe all vertices in V satisfying **OR1** and **OR2**. As can be seen, this also gives an intuitive formulation for control networks. However, for the general case, Haynes *et al*. have shown the NP-hardness of PDS, which is also the case for bipartite and chordal graphs; as noted above, PDS is also only $\Theta(\log n)$-approximable with recent results by Aazami bounding this to a factor of $2^{\log^{1-\epsilon} n}$ [15] unless $\mathrm{NP} \subseteq \mathsf{DTIME}(n^{\mathrm{polylog}(n)})$, and the parameterised intractability results for DS imply $W[2]$-hardness [16]. Moreover, PDS is a non-local problem in that correctness of PDS cannot be checked by only considering a graph neighbourhood, and while it is polynomial-time solvable for max-degree 2 graphs, the best current result for cubic graphs due to Binkele-Raible and Fernau is exponential (in polynomial space) [17]. Guo *et al*. give complexity results for a number of graph classes including circle, planar, split, and partial k-tree graphs [16], while Pai *et al*. give recent results on grid graphs [18] and Atkins *et al*. on block graphs [19]. We now give pseudocode for a simple algorithm to determine the DS based on **OR1** in algorithm 2.1:

Algorithm 2.1: OR1 ($G(V,E)$)

output ($DS = \{v_i, \ldots, v_k\}$ *where* $0 \leq i \leq |V|$)

Choose vertex $v \in V$
$DS \leftarrow \{v\}$ *and* $N(DS) \leftarrow \{v_i, \ldots, v_k\}\ \forall\, i \leq j \leq k / (v, v_j) \in E$
while $V - (DS \cup N(DS)) \neq \emptyset$
do
- *Choose vertex* $w \in V - (DS \cup N(DS))$; $\Longleftarrow$
- $DS \leftarrow DS \cup \{w\}$
- $N(DS) \leftarrow N(DS) \cup \{v_i, \ldots, v_k\}$ *where* $\forall\, i \leq j \leq k \setminus (w, v_j) \in E$;

return (DS)

The PDS algorithm 2.2 is analogously derived from **OR2**:

Algorithm 2.2: OR2 (DS)

output ($N_D = \{v_i, \ldots, v_k\}$ *where* $|N_D| \geq |DS|$)

$N_D \leftarrow DS$;
$i \leftarrow 1$;
while $i \leq |N_D|$
do
  Choose vertex $w \in N_D$ *with degree* $d \geq 2$;
  if ($d-1$ *vertices* $\in N(w)$ *and* $\subseteq N_D$) **and**
  ($\exists$ *vertex* $w_1 \in U$ *where* $w_1 \in N(w)$)
  then
    $N_D \leftarrow N_D \cup \{w_1\}$;
    $U \leftarrow U \setminus \{w_1\}$;
    $i \leftarrow 1$;
  else $\{i \leftarrow i + 1$;
return (PDS)

3 Network and Attack Models

We now describe the graph classes and variants studied subsequently along with the variants of algorithm 2.1 and several attack strategies:

3.1 Network Models

As a baseline we consider the Erdős-Renyi (ER) random graph class [20], often constructed as $ER(n,p)$ with n vertices where each edge included in the graph is determined independently with probability p, as this has also been studied intensively for other approaches described in section 2.

We also consider the simple Watts-Strogatz (WS) random graph model [21], which is given as a construction beginning with a ring lattice of n vertices connected to k neighbours as determined by path lenghts, and with independent probability p choosing an edge of the graph where one vertex to which the edge is incident is chosen uniformly at random, but disallowing duplicate edges (ensuring the graph is simple). These so-called "small world" networks are connected, and have a vertex distance of $\frac{\log n}{\log z}$ (where z is the vertex mean degree), but unlike the Erdős-Renyi random graph exhibit significant clustering, making it an appropriate model e.g. for social networks where the degree distribution following a Dirac delta function centered on the median degree K is suitable. For a considerable number of networks, however, this is not the case, and we chose to include the popular Barabási-Albert (BA) model exhibiting a power-law degree distribution [22]. A construction giving a BA random graph starts with an initial graph of at least 2 vertices with degree ≥ 1 and proceeds to add vertices where each new vertex is connected to existing ones with a probability proportional to the number of edges that existing vertices have of $p_i = \frac{k_i}{\sum_{1 \leq j \leq m} k_j}$ where k_j is the degree of vertex i and m the number of vertices at the time that vertex i is added. The resulting degree distribution follows a power law, giving a small number of nodes with high degree. Empirical studies by Cohen *et al*. give an exponent between 2 and 3 when analysing a number of actual networks, which also have a small diameter $d \sim \ln\ln n$ [23] and a low vertex clustering coefficient. Finally, we also study a further power-law graph model (PLOD), but with lower clustering coefficient [24]. As noted in section 2, we require connected acyclical graphs without self-loops following Lin's structural controllability theorem.

3.2 Vertex Choices

The rules **OR1**,**OR2** do not identify a single power dominating set (or set of driver nodes N_D) for a given graph; we therefore have chosen three generation strategies:

1. Beginning with a vertex of *maximum out-degree*,

2. beginning with a vertex of *minimum out-degree*, and
3. randomly choosing an initial vertex

We note that these also do not identify unique sets for given graph instances. For simplicity, we describe strategies based on algorithm 2.1 satisfying **OR1**. For a given *strategy* we assume that an instance $\mathbf{N}_D^{strategy}$ is represented by a partial order given by the out-degree ($\leq$ or $\geq$) in case of $\mathbf{N}_D^{\max}$ or $\mathbf{N}_D^{\min}$, respectively; in case of $\mathbf{N}_D^{\text{rand}}$, no such relation exists; however, we do assume vertices to be enumerated regardless of the above in the following for each individual instance as we will need to reason over specific instances in the following section.

$\mathbf{N}_D^{\max}$ Obtains N_D based on vertices with maximum out-degree, defining a vertex choice sequence generating the set of *DS* for **OR1**. All vertices with maximum degree d are considered before those with degree $d' < d$ following **OR1** (see algorithm 3.1).

$\mathbf{N}_D^{\min}$ Generates N_D analogous to $\mathbf{N}_D^{\max}$, but using vertices ($\in W$) with the minimum out-degree d until these are exhausted before identifying nodes with degree $d' > d$ (see algorithm 3.1).

$\mathbf{N}_D^{\text{rand}}$ Obtains N_D satisfying **OR1** defined in algorithm 2.1 in which the set of *DS* is generated by randomly choosing a vertex $v \in V$ in each iteration.

3.3 Attack Models

The strategies defined in section 3.2 for obtaining N_D are analysed according to five attack models (denoted here as $\mathbf{AM}_i$) described below. For the analysis, we assume that the attacker has full knowledge of the network and N_D, and will seek to remove vertices from N_D but cannot remove arbitrary numbers of vertices. In this paper we study five different models (see also algorithm 4.1):

$\mathbf{AM}_1$ This strategy attacks the first driver node v in a given ordered set $\mathbf{N}_D^{\text{strategy}}$. The attack consists of removing edges until isolating v from the network, which may also result in isolating several vertices with dependence (i.e. also control relation) on v or partitioning of the underlying graph.

$\mathbf{AM}_2$ Seeks to delete vertices $v \in$ PDS positioned in the middle of the ordered set obtained for a given $\mathbf{N}_D^{\text{strategy}}$.

$\mathbf{AM}_3$ Removes last element v in ordered set given by $\mathbf{N}_D^{\text{strategy}}$.

$\mathbf{AM}_4$ Removes vertices $v \in V$ with highest *betweenness centrality* of the graph.

$\mathbf{AM}_5$ Randomly deletes a vertex $v \in V$ not within $\mathbf{N}_D^{\text{strategy}}$ in order to analyse the behaviour of the entire graph after the isolation/removal of the target v.

Algorithm 3.1: MAXIMUM/MINIMUM STRATEGIES FOR OR1 ($G(V,E)$)

output ($DS = \{v_i, \ldots, v_k\}$ *where* $0 \leq i \leq |V|$ *with max./min. out-degree*);

$d \leftarrow$ *Obtain max./min. out-degree in* V;
$DS \leftarrow \{\}$; $N(DS) \leftarrow \{\}$;
while $(V - (DS \cup N(DS)) \neq \emptyset)$
do
- $W \leftarrow$ *Obtain the set of vertices* $\in V$ *of degree* d;
- **for each** $w \in W$(*chosen randomly*)
  - **do**
    - **if** $w \notin (DS \cup N(DS))$
      - **then** $DS \leftarrow DS \cup \{w\}$;
        $N(DS) \leftarrow N(DS) \cup \{z_i, \ldots, z_k\}\ \forall\, i \leq j \leq k \setminus (w, z_j) \in E$;
- $d \leftarrow$ *Update d with next-smaller/-larger out-degree in* V;

return (DS)

4 Structural Controllability under Vertex Removal

To evaluate the three types of structural controllability strategies ($\mathbf{N}_D^{\max}$, $\mathbf{N}_D^{\min}$ and $\mathbf{N}_D^{\text{rand}}$) described in section 3.2, several attack patterns were studied for the graph topologies described in section 3.1. As large-scale networks are of particular interest, networks with $50\ldots2000$ vertices were studied. The focus has been on *sparse* graphs that are representative of critical infrastructures such as power networks, this is reflected in the parameter choice for the different topologies (e.g. $p_k = 0.3$ in ER/WS; $d^- = 2$ in BA for $\alpha \approx 3$). Under these conditions, robustness is evaluated from two perspectives:

1. *degree of connectivity*, and
2. *degree of observability*.

For the former case, diameter (Dm), density, and average clustering coefficient (CC) are considered. These values should maintain small values in proportion to the growth and the average degree of links (AD), and more specifically after an attack. For observability, we consider the remaining observable network as a percentage (**OR1**).

Algorithm 4.1: ATTACK MODELS $(\mathscr{G}(V,E), AM, \mathbf{N}_D^{\text{strategy}})$

```
output (Isolation of a vertex for a given 𝒢(V,E));
local target ← 0;

if AM == AM_1
  then {target ← N_D^strategy[1];
  else { if AM == AM_2
           then {target ← N_D^strategy[(SIZE(N_D^strategy))/2];
           else { if AM == AM_3
                    then
                  {target ← N_D^strategy[(SIZE(N_D^strategy))];
                  else { if AM == AM_4
                           then
                         {target ← BETWEENNESS CENTRALITY(𝒢(V,E));
                           else {target ← OUTSIDE N_D^strategy(𝒢(V,E), N_D^strategy);
ISOLATE VERTEX(𝒢(V,E), target);
return (𝒢(V,E))
```

The diameter for ER graphs remains broadly stable for larger numbers of nodes as is well-known; however, the density and CC (see figures 1 and 2) for small networks (with $50\ldots500$ vertices) is significantly reduced after the attack. This reduction is even more notable when the perturbation is targeted, i.e. to locations with maximum out-degree ($\mathbf{AM}_1$ on $\mathbf{N}_D^{\max}$, $\mathbf{AM}_3$ on $\mathbf{N}_D^{\min}$) or with the highest betweenness centrality inside the network ($\mathbf{AM}_4$ on $\mathbf{N}_D^{\max}$, $\mathbf{N}_D^{\max}$, and $\mathbf{N}_D^{\text{rand}}$). With a similar behaviour for small networks, WS topology behaviour may appear somewhat confusing as it does not fully capture small-world behaviour in which network diameter is significant. The reason for this lies in the fact that we work with small connectivity probabilities ($p_k = 0.3$) where the average degree of links reaches small values (≈ 2) regardless the network dimension (see table 1). On the other hand, although table 1 and figure 2 also highlight that small WS networks lose diameter values and CC with respect to the initial network, this does not affect to the global network density. Therefore, this type of topology is resilient to PDS vertex isolation, and more particularly to those vertices with the maximum out-degree or with the highest betweenness centrality.

For power-law distributions, parameters for BA distributions remain almost invariant for both small networks and large networks (cf. figures 3 and 4), confirming overall resilience but some sensitivity in observability (table 3) to attacks of type $\mathbf{N}_D^{\max}$ on small networks (50 nodes). Table 3 shows the fraction of

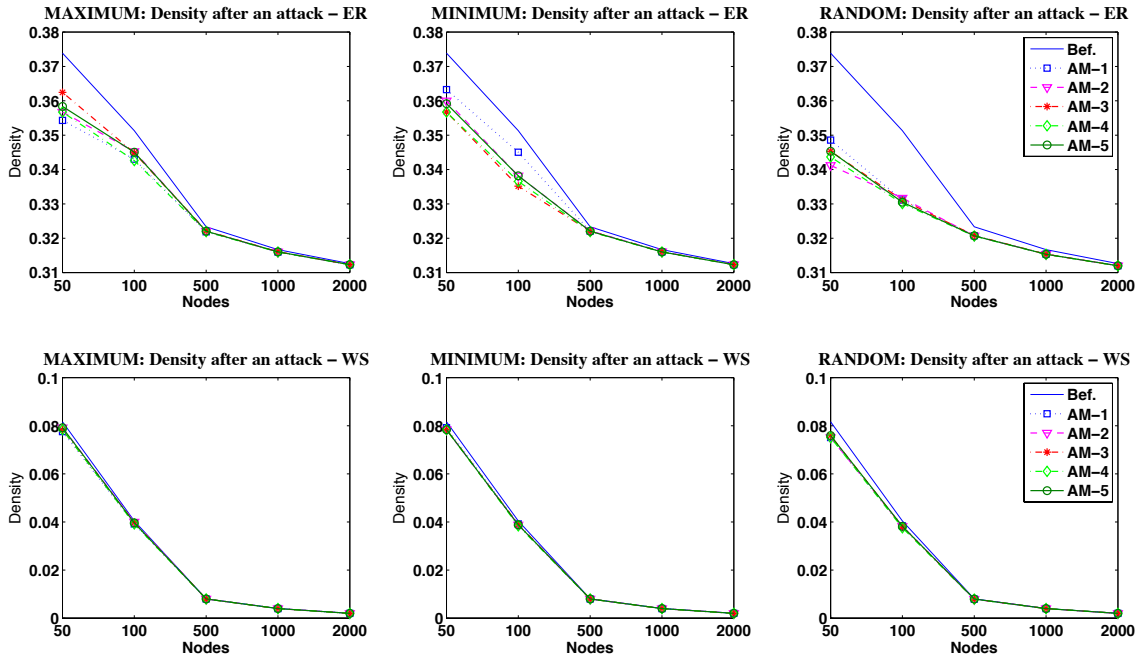

Figure 1: Global density after attack in ER and WS networks

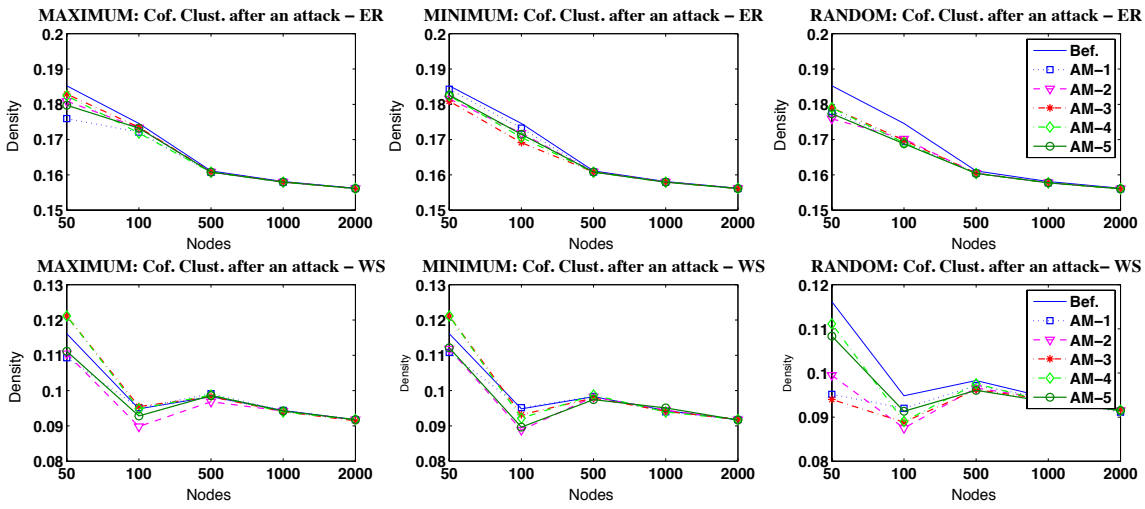

Figure 2: Clustering coefficient after attack in ER and WS networks

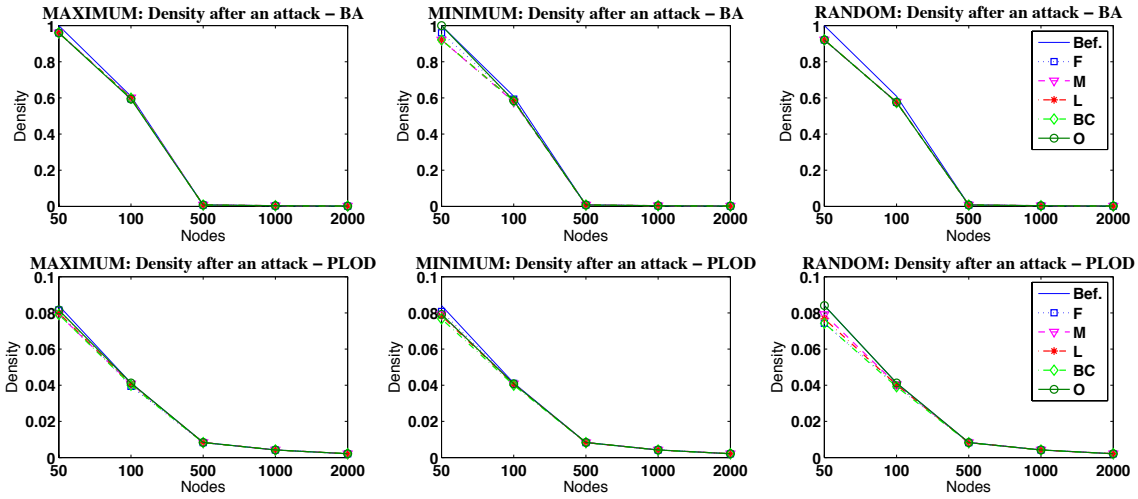

Figure 3: Global density after attack in BA and low-exponent power-law networks

observed nodes for each topology and shows observability remaining high ($\simeq$ 90% and 100% of observability) after attack. Similar to the base BA distribution, low-exponent power-law networks appear robust except to $\mathbf{AM}_4$ attacks where the network diameter varies for any distribution (50…2000) when the node with the highest centrality is targeted. In contrast, $\mathbf{AM}_5$ attacks do not present major risks with respect to intentional threats, but can have an impact on observability with 90% of observation in the worst case. This means that observability is a factor not only dependent on the network topology and construction strategies of driver nodes ($\mathbf{N}_D^{\max}$, $\mathbf{N}_D^{\max}$ and $\mathbf{N}_D^{\text{rand}}$), but also on the nature of the attack or perturbation [5] where degree-based attacks are more significant.

		ER					**WS**					**BA** with $alpha \simeq 3$					**PLOD with** $\alpha \simeq 0.3$				
		50	100	500	1000	2000	50	100	500	1000	2000	50	100	500	1000	2000	50	100	500	1000	2000
		Before Attack																			
	DA	6.66	17.39	80.03	157.86	312.17	1.66	2.00	1.97	1.99	1.99	24.50	30.16	1.97	1.99	1.99	2.06	2.04	2.08	2.10	2.11
	Dm	3	4	5	5	5	12	14	38	78	78	1	4	9	11	13	6	12	28	35	46
		AM_1																			
$N_D^{\max}$	**Dm**	3	4	5	5	5	12	16	38	78	78	1	4	9	11	13	6	12	28	35	46
$N_D^{\min}$	**Dm**	3	4	5	5	5	12	14	38	78	78	1	4	9	11	13	6	12	28	35	46
N_D^{rand}	**Dm**	3	4	5	5	5	12	14	39	68	78	1	4	9	11	13	7	12	28	35	46
		AM_2																			
$N_D^{\max}$	**Dm**	4	4	5	5	5	12	14	38	78	78	1	4	9	11	13	6	12	28	35	46
$N_D^{\min}$	**Dm**	3	4	5	5	5	12	14	37	78	78	1	4	9	11	13	6	12	28	35	46
N_D^{rand}	**Dm**	3	4	5	5	5	12	14	39	78	78	6	6	9	11	13	6	12	28	35	46
		AM_3																			
$N_D^{\max}$	**Dm**	3	4	5	5	5	9	14	38	78	78	1	4	9	11	13	7	12	28	35	46
$N_D^{\min}$	**Dm**	4	4	5	5	5	9	14	38	78	78	1	4	9	11	13	6	12	28	35	46
N_D^{rand}	**Dm**	3	4	5	5	5	12	16	39	78	78	1	4	9	11	13	6	11	28	35	46
		AM_4																			
$N_D^{\max}$	**Dm**	4	4	5	5	5	9	15	45	78	78	1	4	9	11	13	8	11	25	33	51
$N_D^{\min}$	**Dm**	4	4	5	5	5	9	15	45	78	78	1	4	9	11	13	9	11	25	33	51
N_D^{rand}	**Dm**	4	4	5	5	5	9	15	45	78	78	1	4	9	11	13	9	11	25	33	51
		AM_5																			
$N_D^{\max}$	**Dm**	4	4	5	5	5	12	14	38	78	78	1	4	9	11	13	6	12	28	35	46
$N_D^{\min}$	**Dm**	4	4	5	5	5	12	14	38	78	78	1	4	9	11	13	6	12	28	35	46
N_D^{rand}	**Dm**	3	4	5	5	5	12	16	39	78	78	1	4	9	11	13	6	12	28	35	46

Table 1: Network diameter before and after a perturbation or attack

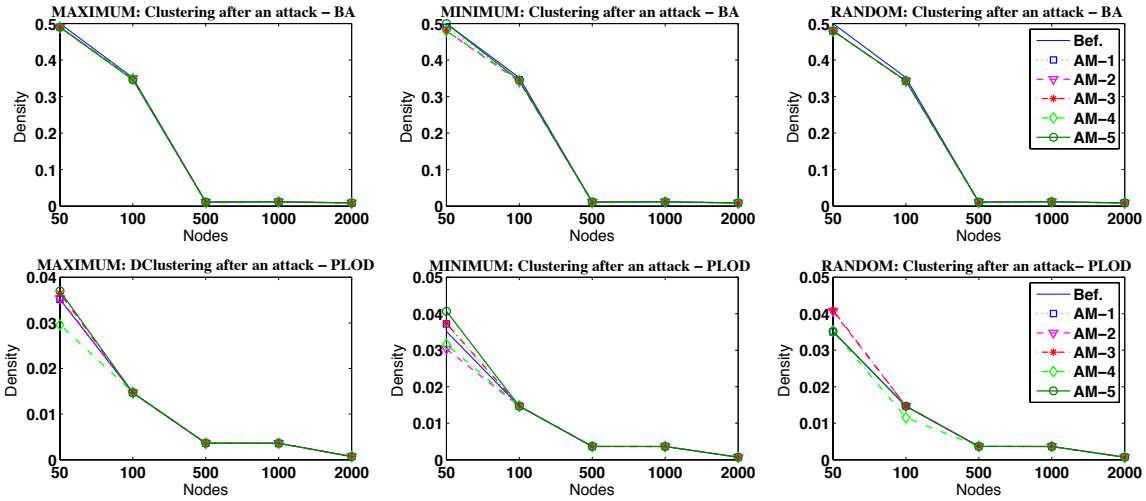

Figure 4: Local density after attack low-exponent power-law networks

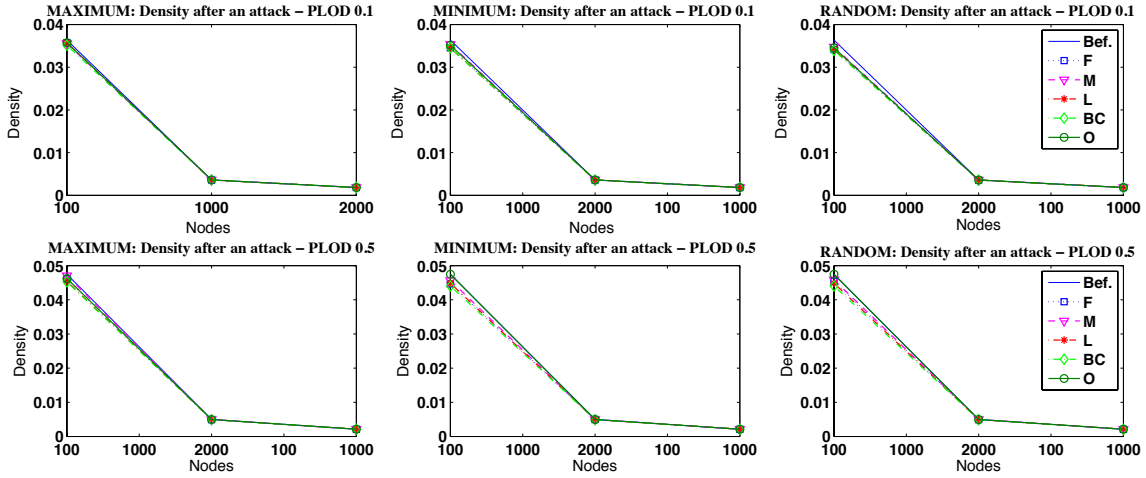

Figure 5: Global density after attack low-exponent power-law networks

Varying the exponent of the power-law distribution (α = 0.1, 0.3 and 0.5), we observe no significant change in global density after perturbation (cf. figures 3 and 5), even when the diameter vary after an **AM-4** threat with respect to the rest of threats (see table 2); a relevant datum highlighting the above analysis. Even so, tables 3 and 2 show that the observation percentage remains high with varying exponents independent of connectivity.

	Diameter						CC						Observation Rate					
	PLOD $\alpha \simeq 0.1$			PLOD $\alpha \simeq 0.5$			PLOD $\alpha \simeq 0.1$			PLOD $\alpha \simeq 0.5$			PLOD $\alpha \simeq 0.1$			PLOD $\alpha \simeq 0.5$		
	100	1000	2000	100	1000	2000	100	1000	2000	100	1000	2000	100	1000	2000	100	1000	2000
	AM_1																	
N_D^{max}	10	36	36	14	25	46	0.0152	0.0028	0.0013	0.0192	0.0036	0.0007	99.0	99.7	99.9	98.0	99.7	100.0
N_D^{min}	10	36	36	14	25	46	0.0162	0.0028	0.0013	0.0169	0.0039	0.0007	100.0	99.8	99.85	100.0	99.8	100.0
N_D^{rand}	9	36	36	14	23	46	0.0180	0.0028	0.0013	0.0176	0.0036	0.0007	100.0	99.9	99.9	100.0	99.8	100.0
	AM_2																	
N_D^{max}	10	36	36	14	25	46	0.0136	0.0028	0.0013	0.0198	0.0039	0.0007	99.0	99.7	99.9	98.0	99.9	100.0
N_D^{min}	10	36	36	14	25	46	0.0153	0.0028	0.0013	0.0195	0.0039	0.0007	100.0	99.8	99.85	100.0	99.8	100.0
N_D^{rand}	9	36	36	14	25	46	0.0155	0.0028	0.0013	0.0187	0.0039	0.0007	100.0	99.9	99.9	100.0	99.8	100.0
	AM_3																	
N_D^{max}	10	36	36	14	25	46	0.0123	0.0028	0.0013	0.0179	0.0039	0.0007	99.9	99.7	99.9	98.0	99.9	100.0
N_D^{min}	12	36	36	14	25	46	0.0146	0.0028	0.0013	0.0181	0.0039	0.0007	100.0	99.8	99.85	100.0	99.8	100.0
N_D^{rand}	10	36	36	14	23	46	0.0158	0.0028	0.0013	0.0181	0.0039	0.0007	100.0	99.9	99.9	100.0	99.8	100.0
	AM_4																	
N_D^{max}	12	36	38	11	26	51	0.0145	0.0028	0.0013	0.0162	0.0037	0.0007	99.0	99.7	99.9	97.0	99.9	100.0
N_D^{min}	12	36	38	11	26	51	0.0146	0.0028	0.0013	0.0151	0.0037	0.0007	100.0	99.8	99.85	100.0	99.8	100.0
N_D^{rand}	11	36	38	11	26	51	0.0148	0.0028	0.0013	0.0151	0.0037	0.0007	1000.0	99.9	99.9	100.0	99.8	100.0
	AM_5																	
N_D^{max}	10	36	36	14	25	46	0.0153	0.0028	0.0013	0.0187	0.0039	0.0007	99.0	99.7	99.85	97.0	99.8	99.95
N_D^{min}	10	36	36	14	23	46	0.0155	0.0028	0.0013	0.0198	0.0039	0.0007	99.0	99.8	99.8	100.0	99.8	99.95
N_D^{rand}	10	36	36	14	23	46	0.0158	0.0028	0.0013	0.0198	0.0039	0.0007	99.0	99.8	99.85	100.0	99.7	99.95

Table 2: Diameter and observation rate for a varied exponentiation of PLOD

5 Conclusions

In this paper we have analysed the robustness of power-dominating sets (PDS) determining the controllability of a network on a number of network topologies including elementary *Erdös-Renyi* random graphs as well as the small-world *Watts-Strogatz* models and several scale-free networks including the *Barabási-Albert* model and particularly power-law networks which approximate structures e.g. found in power networks [25]. We have studied the effects of several non-interactive attack types on the PDS and underlying graphs, showing even limited *targeted* attacks to be highly disruptive in connectivity terms in power-law and small-world networks, or in observability terms in scale-free networks. Ongoing and future work extends this analysis to *interactive* and *concurrent attacks* and the development of efficient stabilisation mechanisms preserving domination properties and hence controllability for the types of graph studied here as little is presently known for these highly relevant classes [16].

	ER					WS					BA with $\alpha \simeq 3$					PLOD with $\alpha \simeq 0.3$				
	50	100	500	1000	2000	50	100	500	1000	2000	50	100	500	1000	2000	50	100	500	1000	2000
	AM_1																			
N_D^{max}	92.0	86.0	99.8	99.5	99.95	96.0	89.0	99.8	99.7	99.9	20.0	97.0	100.0	100.0	100.0	98.0	100.0	100.0	99.6	100.0
N_D^{min}	100.0	100.0	100.0	100.0	100.0	100.0	98.0	100.0	100.0	100.0	100.0	99.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
N_D^{rand}	92.0	96.0	98.4	99.5	99.8	96.0	98.0	96.2	97.8	97.85	94.0	96.0	99.8	99.8	99.9	100.0	100.0	100.0	100.0	100.0
	AM_2																			
N_D^{max}	100.0	86.0	100.0	99.8	99.9	100.0	90.0	99.80	99.9	99.95	20.0	95.0	100.0	100.0	100.0	98.0	100.0	100.0	100.0	100.0
N_D^{min}	100.0	100.0	100.0	100.0	100.0	100.0	98.0	100.0	99.9	100.0	100.0	99.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
N_D^{rand}	88.0	98.0	98.4	99.3	99.85	96.0	98.0	96.2	97.8	97.85	94.0	96.0	99.8	99.8	99.9	100.0	100.0	100.0	100.0	100.0
	AM_3																			
N_D^{max}	100.0	91.0	100.0	99.9	100.0	100.0	91.0	100.0	99.9	100.0	20.0	96.0	100.0	100.0	100.0	98.0	100.0	100.0	100.0	100.0
N_D^{min}	100.0	100.0	99.8	99.9	99.95	98.0	98.0	100.0	100.0	100.0	100.0	99.0	100.0	100.0	99.95	100.0	100.0	100.0	100.0	100.0
N_D^{rand}	86.0	96.0	98.0	99.3	99.8	96.0	98.0	96.2	97.8	97.85	92.0	96.0	99.8	99.8	99.9	100.0	100.0	100.0	100.0	100.0
	AM_4																			
N_D^{max}	98.0	90.0	99.8	99.9	99.95	100.0	91.0	99.8	100.0	99.95	20.0	97.0	100.0	100.0	100.0	98.0	100.0	100.0	100.0	100.0
N_D^{min}	100.0	99.0	99.8	99.9	99.95	98.0	98.0	99.8	100.0	99.95	100.0	98.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
N_D^{rand}	90.0	97.0	98.2	99.3	99.75	96.0	98.0	96.2	97.8	97.85	92.0	95.0	99.8	99.8	99.9	100.0	100.0	100.0	100.0	100.0
	AM_5																			
N_D^{max}	98.0	90.0	99.8	99.9	99.95	98.0	90.0	99.8	99.9	99.95	50.0	95.0	100.0	100.0	100.0	98.0	100.0	99.8	100.0	99.95
N_D^{min}	98.0	99.0	99.8	99.9	99.95	98.0	98.0	99.8	99.9	99.95	100.0	98.0	100.0	100.0	100.0	98.0	99.0	99.8	100.0	99.95
N_D^{rand}	90.0	96.0	98.4	99.3	99.8	96.0	97.0	96.2	97.8	97.85	96.0	96.0	99.6	99.8	99.85	100.0	100.0	99.8	100.0	99.95

Table 3: Observation rate after perturbation or attack

Acknowledgements *The authors would like to acknowledge contributions by A. Baiocco to simulations. Research of C. Alcaraz was funded by the Marie Curie COFUND programme "U-Mobility" co-financed by University of Málaga and the EU 7th FP (GA 246550). Research by A. Baiocco and S. Wolthusen is based in part upon work supported by the 7th Framework Programme of the European Union Joint Technology Initiatives Collaborative Project ARTEMIS under Grant Agreement 269374 (Internet of Energy for Electric Mobility).*

References

[1] R. E. Kalman. Mathematical description of linear dynamical systems. *Journal of the Society of Industrial and Applied Mathematics Control Series A*, 1:152–192, 1963.

[2] C.-T. Lin. Structual Controllability. *IEEE Transactions on Automatic Control*, 19(3):201–208, June 1974.

[3] Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási. Controllability of Complex Networks. *Nature*, 473:167–173, May 2011.

[4] W.-X. Wang, X. Ni, Y.-C. Lai, and C. Grebogi. Optimizing controllability of complex networks by minimum structural perturbations. *Physical Review E*, 85(2):026115, February 2012.

[5] C.-L. Pu, W.-J. Pei, and A. Michaelson. Robustness analysis of network controllability. *Physica A: Statistical Mechanics and its Applications*, 391(18):4420–4425, Sep. 2012.

[6] R. G. Downey and M. R. Fellows. *Parameterized Complexity*. Monographs in Computer Science. Springer-Verlag, Heidelberg, Germany, 1999.

[7] S. Micali and V. V. Vazirani. An $O(\sqrt{|V|}|E|)$ Algorithm for Finding Maximum Matching in General Graphs. In Ronald V. Book, editor, *Proceedings of the 21st Annual Symposium on Foundations of Computer Science (FOCS 1980)*, pages 17–27, Syracuse, NY, USA, October 1980. IEEE Press.

[8] L. Lovász and M. D. Plummer. *Matching Theory*. American Mathematical Society, Providence, RI, USA, 2009.

[9] M. Pósfai, Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási. Effect of Correlations on Network Controllability. *Nature Scientific Reports*, 3(1067):1–7, January 2013.

[10] B. Bollobás and O. Riordan. Robustness and Vulnerability of Scale-Free Random Graphs. *Internet Mathematics*, 1(1):1–35, January 2003.

[11] B. Sudakov and V. H. Vu. Local Resilience of Graphs. *Random Structures & Algorithms*, 33(4):409–433, August 2008.

[12] T. W. Haynes, S. Mitchell Hedetniemi, S. T. Hedetniemi, and M. A. Henning. Domination in Graphs Applied to Electric Power Networks. *SIAM Journal on Discrete Mathematics*, 15(4):519–529, August 2002.

[13] U. Feige. A Threshold of $\ln n$ for Approximating Set Cover. *Journal of the ACM*, 45(4):634–652, July 1998.

[14] J. Kneis, D. Mölle, S. Richter, and P. Rossmanith. Parameterized Power Domination Complexity. *Information Processing Letters*, 98(4):145–149, May 2006.

[15] A. Aazami and K. Stilp. Approximation Algorithms and Hardness for Domination with Propagation. *SIAM Journal on Discrete Mathematics*, 23(3):1382–1399, Sep. 2009.

[16] J. Guo, R. Niedermeier, and D. Raible. Improved Algorithms and Complexity Results for Power Domination in Graphs. *Algorithmica*, 52(2):177–202, October 2008.

[17] D. Binkele-Raible and H. Fernau. An Exact Exponential Time Algorithm for POWER DOMINATING SET. *Algorithmica*, 63(1–2):323–346, June 2012.

[18] K.-J. Pai, J.-M. Chang, and Y.-L. Wang. Restricted Power Domination and Fault-Tolerant Power Domination on Grids. *Discrete Applied Mathematics*, 158(10):1079–1089, 2010.

[19] D. Atkins, T. W. Haynes, and M. A. Henning. Placing Monitoring Devices in Electric Power Networks Modelled by Block Graphs. *Ars Combinatorica*, 79(1), April 2006.

[20] B. Bollobás. *Random Graphs*, volume 73 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, UK, 2nd edition, 2001.

[21] D. J. Watts and S. H. Strogatz. Collective Dynamics of 'Small-World' Networks. *Nature*, 393:440–442, June 1998.

[22] R. Albert and A.-L. Barabási. Statistical Mechanics of Complex Networks. *Reviews of Modern Physics*, 74(1):47–97, July 2002.

[23] R. Cohen, S. Havlin, and D. ben Avraham. Structural Properties of Scale-Free Networks. In S. Bornholdt and H.-G. Schuster, editors, *Handbook of Graphs and Networks: From the Genome to the Internet*. Wiley-VCH, Weinheim, Germany, 2005.

[24] C. R. Palmer and J. G. Steffan. Generating Network Topologies That Obey Power Laws. In *Proceedings of the 2000 IEEE Global Telecommunications Conference (GLOBECOM '00)*, volume 1, pages 434–438, San Francisco, CA, USA, November 2000. IEEE Press.

[25] G. A. Pagani and M. Aiello. The Power Grid as a Complex Network: A Survey. *Physica A: Statistical Mechanics and its Applications*, 392(11):2688–2700, June 2013.