Structural Controllability of Networks for Non-Interactive Adversarial Vertex Removal

C. Alcaraz[1,4], *E. Etchevés Miciolino*[2] *and S. Wolthusen*[3,4]

[1]Computer Science Department, University of Málaga, Spain
[2]Complex Systems & Security Laboratory,
Universitá Campus Bio-Medico di Roma, Italy
[3]Norwegian Information Security Laboratory, Gjøvik University College, Norway
[4]Information Security Group, Royal Holloway, University of London, UK

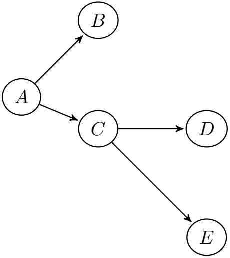
alcaraz@lcc.uma.es
e.etcheves@unicampus.it
stephen.wolthusen@hig.no

September 18th 2013

Contents

Controllability theory and Motivation

- 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.**



Controllability theory and Motivation

- Controllability theory was introduced by Kalman through:

$$\dot{x}(t) = Ax(t) + Bu(t), \quad x(t_0) = x_0$$

where:

  - $x(t)$ is the vector of current states with n nodes at time t;
  - **A** is an adjacency matrix $n \times n$ giving the network topology;
  - **B** an *input* matrix $n \times m$, where $m \leq n$, identifying the set of nodes controlled; and
  - $u(t) = (u_1(t), \ldots, u_m(t))$, the *input vector* which forces the system to a desired state.

- A system is *controllable* if the *controllability matrix* $[B, AB, A^2B, \ldots A^{n-1}B]$ = n, i.e., it has full rank.

But:

- How can we represent large networks with hundreds and thousands nodes using this mathematical formulation?

Controllability and Motivation

Through graph theory is possible to simplify the **control over networks**, introducing the concept of structural controllability. Let $\mathscr{G}(A,B) = (V,E)$ a digraph,

- $E = E_A \cup E_B$ the set of edges;
- $V = V_A \cup V_B$ is the set of vertices; and
- V_B represents **the minimum driver node subset $\mathbf{N}_D$** in charge of helping the system reach a desired configuration from an arbitrary configuration in a finite number of steps.

$\mathbf{N}_D$ can be obtained through the **POWER DOMINATING SET** (PDS) problem.

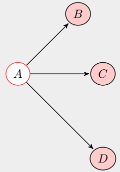
- The PDS problem was introduced for monitoring electric power networks, as an extension of the Dominating Set (DS) problem
- The problem can be simplified by **two observation rules**

Power Domination

Observation Rules

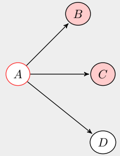
OR1

A vertex in the $\mathbf{N}_D$ observes itself and all its neighbours



OR2

In an observed vertex v with out-degree $d \geq 2$ is adjacent to $d-1$ observed vertices, then the remaining unobserved vertex becomes observed as well



Observation Rules - OR1

Algorithm 2.1: OR1 ($\mathscr{G}(V,E)$)

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 $V - (DS \cup N(DS)) \neq \oslash$

$$\textbf{do} \begin{cases} \textit{Choose vertex } w \in V - (DS \cup N(DS)); \Longleftarrow \\ DS \leftarrow DS \cup \{w\} \\ N(DS) \leftarrow N(DS) \cup \{v_i, \ldots, v_k\} \textit{ where } \forall\, i \leq j \leq k \setminus (w, v_j) \in E; \end{cases}$$

return (DS)

Observation Rules - OR2

Algorithm 2.2: OR2 (DS)

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

$N_D \leftarrow DS$;
$i \leftarrow 1$;
while $i \leq |N_D|$

do $\left\{\begin{array}{l} \textit{Choose vertex } w \in N_D \textit{ with degree } d \geq 2; \\ \textbf{if } (d-1 \textit{ vertices } \in N(w) \textit{ and } \subseteq N_D) \textbf{ and} \\ (\exists \textit{ vertex } w_1 \in U \textit{ where } w_1 \in N(w)) \\ \quad \textbf{then } \left\{\begin{array}{l} N_D \leftarrow N_D \cup \{w_1\}; \\ U \leftarrow U \setminus \{w_1\}; \\ i \leftarrow 1; \\ \quad \textbf{else } \{i \leftarrow i + 1; \end{array}\right. \end{array}\right.$

return (PDS)

Generation Strategies of PDS

Three generation strategies have been defined taking into account **the vertex choice sequence when generating** *DS* **for OR1**:

- $\mathbf{N}_D^{\mathrm{max}}$ Beginning with the vertex of maximum out-degree;
- $\mathbf{N}_D^{\mathrm{min}}$ Beginning with the vertex of minimum out-degree;
- $\mathbf{N}_D^{\mathrm{rand}}$ Randomly choosing an initial vertex

Generation Strategies of PDS

Three generation strategies have been defined taking into account **the vertex choice sequence when generating** *DS* **for OR1**:

- $\mathbf{N}_D^{\max}$ Beginning with the vertex of maximum out-degree;
- $\mathbf{N}_D^{\min}$ Beginning with the vertex of minimum out-degree;
- $\mathbf{N}_D^{\mathrm{rand}}$ Randomly choosing an initial vertex

Generation Strategies of PDS

Three generation strategies have been defined taking into account **the vertex choice sequence when generating** *DS* **for OR1**:

- $\mathbf{N}_D^{\max}$ Beginning with the vertex of maximum out-degree;
- $\mathbf{N}_D^{\min}$ Beginning with the vertex of minimum out-degree;
- $\mathbf{N}_D^{\mathrm{rand}}$ Randomly choosing an initial vertex

Generation Strategies of PDS

Three generation strategies have been defined taking into account **the vertex choice sequence when generating** *DS* **for OR1**:

- $\mathbf{N}_D^{\mathrm{max}}$ Beginning with the vertex of maximum out-degree;
- $\mathbf{N}_D^{\mathrm{min}}$ Beginning with the vertex of minimum out-degree;
- $\mathbf{N}_D^{\mathrm{rand}}$ Randomly choosing an initial vertex

Generation Strategies of PDS

Three generation strategies have been defined taking into account **the vertex choice sequence when generating** ***DS*** **for OR1**:

- $\mathbf{N}_D^{\mathrm{max}}$ Beginning with the vertex of maximum out-degree;
- $\mathbf{N}_D^{\mathrm{min}}$ Beginning with the vertex of minimum out-degree;
- $\mathbf{N}_D^{\mathrm{rand}}$ Randomly choosing an initial vertex

Therefore

We assume a partial order given by the **out-degree ($\leq$ or $\geq$)** in case of $\mathbf{N}_D^{\mathrm{max}}$ or $\mathbf{N}_D^{\mathrm{min}}$, respectively; in case of $\mathbf{N}_D^{\mathrm{rand}}$, **no** such **relation exists**

But:

- Are these types of control networks robustness against threats?

Network and Attack Models

Network Models

Topologies deployed:

- Random distributions: Erdös-Rényi (ER)
- Small-world distributions: Watts-Strogatz (WS)
- Power-law distributions:
  - Barabási-Albert (BA) with preferential attachment
  - Power-Law Out-Degree (PLOD)

Note that:

Power-law networks present approximated structures to the found in power networks

Attack Models

Five attack models have been developed under the following assumptions:

- Attack a v until isolating it from the network, which may also result in isolating several vertices or partitioning the entire graph.
- The attacker has full knowledge of the topology and of N_D.

Attack Models

Five attack models have been developed under the following assumptions:

- Attack a v until isolating it from the network, which may also result in isolating several vertices or partitioning the entire graph.
- The attacker has full knowledge of the topology and of N_D.

Attack Models

Five attack models have been developed under the following assumptions:

- Attack a v until isolating it from the network, which may also result in isolating several vertices or partitioning the entire graph.
- The attacker has full knowledge of the topology and of N_D.

Attack Models

Then,

- **AM_1** The first driver node v in a given ordered set $\mathbf{N}_D^{\text{strategy}}$
- **AM_2** The driver node positioned in the middle of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM_3** The last node driver of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM_4** The node with the highest *betweenness centrality* of the graph
- **AM_5** A random vertex outside a given $\mathbf{N}_D^{\text{strategy}}$

Attack Models

Then,

- **AM$_1$** The first driver node v in a given ordered set $\mathbf{N}_D^{\text{strategy}}$
- **AM$_2$** The driver node positioned in the middle of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM$_3$** The last node driver of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM$_4$** The node with the highest *betweenness centrality* of the graph
- **AM$_5$** A random vertex outside a given $\mathbf{N}_D^{\text{strategy}}$

Attack Models

Then,

- **AM_1** The first driver node v in a given ordered set $\mathbf{N}_D^{\text{strategy}}$
- **AM_2** The driver node positioned in the middle of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM_3** The last node driver of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM_4** The node with the highest *betweenness centrality* of the graph
- **AM_5** A random vertex outside a given $\mathbf{N}_D^{\text{strategy}}$

Attack Models

Then,

- **AM$_1$** The first driver node v in a given ordered set $\mathbf{N}_D^{\text{strategy}}$
- **AM$_2$** The driver node positioned in the middle of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM$_3$** The last node driver of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM$_4$** The node with the highest *betweenness centrality* of the graph
- **AM$_5$** A random vertex outside a given $\mathbf{N}_D^{\text{strategy}}$

Attack Models

Then,

- **AM_1** The first driver node v in a given ordered set $\mathbf{N}_D^{\text{strategy}}$
- **AM_2** The driver node positioned in the middle of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM_3** The last node driver of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM_4** The node with the highest *betweenness centrality* of the graph
- **AM_5** A random vertex outside a given $\mathbf{N}_D^{\text{strategy}}$

Attack Models

Then,

- **AM_1** The first driver node v in a given ordered set $\mathbf{N}_D^{\text{strategy}}$
- **AM_2** The driver node positioned in the middle of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM_3** The last node driver of a given $\mathbf{N}_D^{\text{strategy}}$
- **AM_4** The node with the highest *betweenness centrality* of the graph
- **AM_5** A random vertex outside a given $\mathbf{N}_D^{\text{strategy}}$

Attack Models

Algorithm 3.1: ATTACK MODELS ($\mathscr{G}G(V,E), AM, \mathbf{N}_D^{\text{strategy}}$)

output (*Isolation of a vertex for a given* $\mathscr{G}(V,E)$);
local *target* $\leftarrow 0$;

if $AM == \mathbf{AM}_1$
  then $\{$ *target* $\leftarrow \mathbf{N}_D^{\text{strategy}}[1]$;
  else $\{$
    if $AM == \mathbf{AM}_2$
      then $\{$ *target* $\leftarrow \mathbf{N}_D^{\text{strategy}}[(\text{SIZE}(\mathbf{N}_D^{\text{strategy}}))/2]$;
      else $\{$
        if $AM == \mathbf{AM}_3$
          then
          $\{$ *target* $\leftarrow \mathbf{N}_D^{\text{strategy}}[(\text{SIZE}(\mathbf{N}_D^{\text{strategy}}))]$;
          else $\{$
            if $AM == \mathbf{AM}_4$
              then
              $\{$ *target* $\leftarrow$ BETWEENNESS CENTRALITY($\mathscr{G}(V,E)$);
              else $\{$ *target* $\leftarrow$ OUTSIDE $\mathbf{N}_D^{\text{strategy}}(\mathscr{G}(V,E), \mathbf{N}_D^{\text{strategy}})$;

ISOLATE VERTEX($\mathscr{G}(V,E)$, *target*);
return ($\mathscr{G}(V,E)$)

Structural Controllability under Vertex Removal

Experimentation

Experimental Design

Goal

To evaluate the behaviour of the three types of structural controllability strategies $\mathbf{N}_D^{\max}$, $\mathbf{N}_D^{\min}$ and $\mathbf{N}_D^{\mathrm{rand}}$ against threats

Experimental Design

Goal

To evaluate the behaviour of the three types of structural controllability strategies $\mathbf{N}_D^{\max}$, $\mathbf{N}_D^{\min}$ and $\mathbf{N}_D^{\text{rand}}$ against threats

Network characteristics

- **Sparse graphs** to represent main critical infrastructures
  - Connectivity probability of $p_k = 0.3$ for ER/WS, $d^- = 2$ for BA for $\alpha \simeq 3$, $alpha = 0.1, 0.3, 0.5$ for PLOD
- Networks with 50, 100, 500, 1000, 2000 nodes

Experimental Design

Goal

To evaluate the behaviour of the three types of structural controllability strategies $\mathbf{N}_D^{\max}$, $\mathbf{N}_D^{\min}$ and $\mathbf{N}_D^{\mathrm{rand}}$ against threats

Network characteristics

- **Sparse graphs** to represent main critical infrastructures
  - Connectivity probability of $p_k = 0.3$ for ER/WS, $d^- = 2$ for BA for $\alpha \simeq 3$, $alpha = 0.1, 0.3, 0.5$ for PLOD
- Networks with 50, 100, 500, 1000, 2000 nodes

Robustness analysis

- ***Connectivity***: Diameter (Dm), density, average cluster coefficient (CC);
- ***Observability***: Percentage of remaining observable network using **OR1**

Degree of Connectivity

Network	Dm	Density	CC	Threat
ER	$\mathbf{N}_{D_{small}}^{\text{max,min,rand}}$	$\mathbf{N}_{D_{small}}^{\text{max,min,rand}*}$	$\mathbf{N}_{D_{small}}^{\text{max}*,\text{min}*,\text{rand}}$	AM_4
WS	$\mathbf{N}_{D}^{\text{max,min,rand}}$	-	$\mathbf{N}_{D_{small}}^{\text{max,min,rand}*}$	$AM_{4,3}$
BA	-	$\mathbf{N}_{D_{small}}^{\text{max,min,rand}}$	$\mathbf{N}_{D_{small}}^{\text{min,rand}}$	-
PLOD-0.1	$\mathbf{N}_{D*}^{\text{max,min,rand}}$	-	$\mathbf{N}_{D_{small}}^{\text{max}*,\text{min,rand}}$	AM_4
PLOD-0.3	$\mathbf{N}_{D*}^{\text{max,min,rand}}$	-	$\mathbf{N}_{D_{small}}^{\text{max,min,rand}*}$	AM_4
PLOD-0.5	$\mathbf{N}_{D*}^{\text{max,min,rand}}$	-	$\mathbf{N}_{D_{small}}^{\text{max,min,rand}}$	AM_4

Degree of Observability

Network	Threat	Rate	Rate
ER	$\forall AM_s$	$\simeq [90 - 100\%]$	$\mathbf{N}_{D_{small}}^{\max*,\min,\text{rand}*}$
WS	$\forall AM_s$	$\simeq [96 - 100\%]$	$\mathbf{N}_{D*}^{\max*,\min,\text{rand}}$
BA	$\forall AM_s$	$\simeq [2 - 100\%]$	$\mathbf{N}_{D_{small}}^{\max**,\min,\text{rand}*}$
PLOD-0.1	$\forall AM_s$	$\simeq [99.40 - 100\%]$	$\mathbf{N}_{D_{small}}^{\max*,\min,\text{rand}}$
PLOD-0.3	$\forall AM_s$	$\simeq [98 - 100\%]$	$\mathbf{N}_{D_{small}}^{\max*,\min,\text{rand}}$
PLOD-0.5	$\forall AM_s$	$\simeq [96 - 100\%]$	$\mathbf{N}_{D_{small}}^{\max*,\min,\text{rand}}$

Conclusions and Future Work

Conclusions

- We review the robustness of power-dominating sets (PDS) determining the controllability for several network topologies
- We studied the effects of several non-interactive attack types on the PDS and underlying graphs
- We conclude that:
  - Limited *targeted* attacks (specially AM_4) are disruptive *in terms of connectivity* for the most of topologies; and
  - in *observability terms* for scale-free networks

Conclusions

- We review the robustness of power-dominating sets (PDS) determining the controllability for several network topologies
- We studied the effects of several non-interactive attack types on the PDS and underlying graphs
- We conclude that:
  - Limited *targeted* attacks (specially AM_4) are disruptive *in terms of connectivity* for the most of topologies; and
  - in *observability terms* for scale-free networks

Conclusions

- We review the robustness of power-dominating sets (PDS) determining the controllability for several network topologies
- We studied the effects of several non-interactive attack types on the PDS and underlying graphs
- We conclude that:
  - Limited *targeted* attacks (specially AM_4) are disruptive *in terms of connectivity* for the most of topologies; and
  - in *observability terms* for scale-free networks

Ongoing and Future Work

- We are currently continuing to investigate further, considering more complex multi-round attack scenarios
- Design and implementation of optimized controllability recovery solutions preserving domination properties, and considering:
  - The hardness of the PDS and its non-locality problem
  - Aspects of optimization through parametrised approximations, with special focus on power-law topologies

Ongoing and Future Work

- We are currently continuing to investigate further, considering more complex multi-round attack scenarios
- Design and implementation of optimized controllability recovery solutions preserving domination properties, and considering:
  - The hardness of the PDS and its non-locality problem
  - Aspects of optimization through parametrised approximations, with special focus on power-law topologies

Cristina Alcaraz
Computer Science Department,
University of Málaga, Spain
Information Security Group, Royal Holloway,
University of London, UK
alcaraz@lcc.uma.es

E. Etchevés Miciolino
Complex Systems & Security Laboratory,
Universitá Campus Bio-Medico di Roma, Italy
e.etcheves@unicampus.it

S. Wolthusen
Norwegian Information Security Laboratory,
Gjøvik University College, Norway
Information Security Group, Royal Holloway,
University of London, UK
stephen.wolthusen@hig.no