Journal of Universal Computer Science, vol. 15, no. 14 (2009), 2747-2764
submitted: 17/3/09, accepted: 30/7/09, appeared: 1/8/09 © J.UCS

Optimal Serverless Networks Attacks, Complexity and some Approximate Algorithms

Carlos Aguirre
(BNG, Computer Engineering Department, Universidad Autónoma de Madrid
28049 Madrid, Spain
Carlos.Aguirre@uam.es)

Ramon Huerta
(Institute for Nonlinear Science, University of California, San Diego, La Jolla
CA, 92093-0402, USA
rhuerta@ucsd.edu)

Lev Tsimring
(Institute for Nonlinear Science, University of California, San Diego, La Jolla
CA, 92093-0402, USA
ltsimring@ucsd.edu)

Abstract: A network attack is a set of network elements that are disabled by an adversary. The goal for the attack is to produce the most possible damage to the network in terms of network connectivity by disabling the least possible number of network elements. We show that the problem of finding the optimal attack in a serverless network is NP-Complete even when only edges or nodes are considered for disabling. We study a node attack policy with polynomial complexity based on shorter paths and show that this attack policy outperforms in most cases classical attacks policies such as random attack or maximum degree attack. We also study the behavior of different network topologies under these attack policies.

Key Words: Network connectivity, Optimal attack problem, NP-Complete, Attack strategies

Category: C.2.1, F.2.2, G.2.2

1 Introduction

An attack is a set of network elements that are disabled by an adversary. The goal of the attack is to disconnect some elements of the network from others. Quasi-optimal attacks for pairs of nodes where only edges can be disabled are found in polynomial time by means of MIN CUT algorithms [Stoer and Wagner 1997]. The resistance of the network and optimal reinforcement against an edge based attack is studied in [Cunningham 1985].

The resistance to node and/or edge based attacks strategies for a given network model (meshes, rings, random, regular, etc) and the study of optimal topologies that present a high resistance to specific attack strategies has been the object of many studies as part of the area of "Survivable networks" [Fortz 2000, Grover 2003]. In [Albert et al. 2000] the tolerance to random failure and maximal degree node disabling is investigated over random networks and Scale-Free (SF) networks from a physics and statistical mechanics point of view. Recently, the stability of multimedia networks under attacks has been studied in [Koukopulos 2009]. In [Leiwo et al. 2000] the problem of finding the minimal set of nodes whose removal produces the maximal damage in terms of connectivity to a single given node is shown to be NP-Complete. The design of fault tolerant networks for arrays and meshes is studied in [Zhang 2000].

In this paper we study the complexity of finding the optimal attack in terms of cost and damage to a serverless network. Serverless networks present specific characteristics, such as the lack of a single centralized authority and many control services are to be maintained in a distributed way. These facts implies that new attack strategies, attack resistant networks and attack damage metrics need to be developed. In this kind of networks the damage of a given attack cannot be measured any more as a function of the connectivity to a single nod, otherwise, the damage of a given attack is usually measured as the size of the biggest connected component of the graph resulting after the attack [Albert et al. 2002, Albert et al. 2000]. In [Abdelouahab et al. 2009] an attack strategy over a particular case of serverless networks, the P2P networks, is studied. Strategies for detecting Distributed Denial of Service flood based attacks have been developed [Li 2004, Li 2006], as in the case of attack strategies, new metrics and methods are needed to develop these strategies for not centralized networks.

In section 2, the exact definitions of serverless communication networks model, attack, cost and damage of an attack and network resistance are provided among other. In section 3 we state precisely the Optimal Attack Problem as the problem of finding an attack that produces a given damage with a cost below a given budget, we also state that such a problem is NP-Complete. In section 4 we provide some approximate attack algorithms, finally, in section 5 we also study the resistance to different node attack policies for several network models: Ring-lattices, Small-World (SW), SF, Random, a mixed model SF-SW and a real graph representing the connectivity of the Western US power grid.

2 Model of Serverless Communication Networks

A *serverless communication network* is a quadruple $CN = \{V, E, c, s\}$ where

1. $V = \{v_1, \cdots, v_{|V|}\}$ is the set of *nodes*,
2. $E = \{e_1, \cdots, e_{|E|}\} : V \times V \to \{0, 1\}$ is the set of *edges*,
3. $c : V \cup E \to \mathbb{Z}_+ \cup \{\infty\}$ is a *cost* function and

4. $s : V \to [0, 1]$ is a *significance function*.

The cost function is a measure of how much it costs to an enemy to disable an element of the network, the infinity value means that the element can't be disabled by any attack. The significance function is an indication of the relevance of the node and therefore how bad is that other elements of the network become disconnected from the node. Cost and significance are *a priori* data over the set of nodes and edges. The cost function could be used, for example, to represent the computational effort or the economical expenses or simply the time needed to disable the node or the edge and the significance function could represent, for example, how many users obtain a denial of a given service (Internet access, data access) in the case that the node is disabled by the attack.

We define an *Attack* $A \subset V \cup E$ over a communication network CN as a set of *disabled* nodes and edges. A *cut* is an attack that succeeds in disconnecting the graph. In a disconnected graph, each maximal set of connected nodes forms a *connected component* of the graph. We define the significance S of a connected component as the sum of the significances of its elements.

$$S(V') = \sum_{i=1}^{|V|} s(v_i) \ with \ v_i \in V' \tag{1}$$

where V' is a connected component of V.

The significance can be calculated for each connected component of the graph. The connected component with the highest significance is named the *core* B_{cc} of the graph. If the graph is connected, the core coincides with the graph. In this paper we assume without loss of generality for our purposes that B_{cc} is unique.

For a given attack A we define arbitrarily the *cost* C of the attack to the communication network CN as the sum of the costs of the elements of CN disabled by the attack A, i.e.

$$C_{CN}(A) = \sum_{i=1}^{|V|+|E|} c(x_i) \ with \ x_i \in A \tag{2}$$

We also define the *damage* D produced in the communication network CN by the attack A as the sum of the significances of the nodes that are disconnected from the core. More formally,

$$D_{CN}(A) = \sum_{i=1}^{|V|} s(v_i) \ with \ x_i \notin B_{cc} \tag{3}$$

We define the *resistance* R of the communication network CN to the attack A as the significance of the elements that are in B_{cc}, this is,

$$R_{CN}(A) = \sum_{i=1}^{|V|} s(v_i) \; with \; v_i \in B_{cc} \tag{4}$$

Finally we define the *efficiency* of an attack A to a communication network CN as:

$$P_{CN}(A) = \frac{D_{CN}(A)}{C_{CN}(A)} \tag{5}$$

3 Optimal attack problem

We can now define the optimal attack problem (OPT_ATTACK) to a serverless network CN in the following terms:

Problem OPT_ATTACK: Given a serverless communication network CN and two fixed values C and D, does there exist an attack A such as $C_{CN}(A) \leq C$ and $D_{CN}(A) \geq D$?

Theorem 1 The OPT_ATTACK problem is NP-Complete even in the case of bidirectional links, $s(v) = 1 \; \forall \; v \in V$, $c(v) = \infty \; \forall \; v \in V$ and $c(e) = 1 \; \forall \; e \in E$. Note that in this case B_{cc} coincides with the biggest connected component of the graph and the significance of a connected component coincides with its size.

Proof We first show that $OPT\_ATTACK \in NP$.

Suppose we are given a communication network CN, an attack A and two numbers C and D. We need to find an algorithm that checks in polynomial time that a given solution solves the problem. We choose as a solution the attack A. The verification algorithm checks that $C_{CN}(A) \leq C$ and $D_{CN}(A) \geq D$ by finding the biggest connected component B_{cc} after the attack. An algorithm of order $O(|E|+|V|log|V|)$ for finding the connected components of a given graph G can be found in [Cormen et al. 1998]. The biggest connected component can be found in time of the order at most $O(|V|)$ and the damage of A can be calculated by adding the size of the remaining connected components in the graph in time of the order at most $O(|V|)$. The program can also compute the cost C of A simply adding the cost of the elements of A. Therefore this verification can be performed in polynomial time.

We prove that OPT_ATTACK is NP-Complete by describing a polynomial reduction to the problem of minimal bisection. The minimal bisection problem consist in finding the minimal set of edges that divide the set of nodes V of a given graph G into two disjoint sets V_1, V_2 such as $|V_1| = |V_2| = |V|/2$ and $V_1 \cup V_2 = V$. The size of the bisection is the number of edges $(v_1, v_2) \in E$ such $v_1 \in V_1 \; and \; v_2 \in V_2$. It can be proved that the minimal bisection problem is NP-Complete [Garey and Johnson 1976].

Now we show that OPT_ATTACK is NP-Complete.

Let us consider the graph $G = (V, E)$ for the minimal bisection problem. Let us construct a new graph G' adding a new extra node s and connecting this new node with each of the $|V|$ nodes of G by $(|V|^2/4) + 1$ routes to each node in G. Each route will consist of an auxiliary node a^i_v $i = 0, \cdots, (|V|^2/4) + 1$, an edge from s to the auxiliary node a^i_v and an edge from a^i_v to node v in the graph. This new graph G' verifies $|V'| = |V|^3/4 + 2|V| + 1$ and $|E'| = |E| + 2(|V|^3/4 + |V|)$.

Now we assign a serverless communication network to the amplified graph G':

- $V' = V \cup \{s\} \cup \{a^i_v | v \in V \ and \ i = 1 \cdots (n^2/4) + 1\}$
- $E' = E \cup \{(s, a^i_v), (a^i_v, s), (v, a^i_v), (a^i_v, v) \mid v \in V \ and \ i = 1 \cdots n^2/4 + 1\}$
- $c(e) = 1 \ if \ e \in E', c(v) = \infty \ if \ v \in V'$
- $s(v) = 1 \ if \ v \in V'$

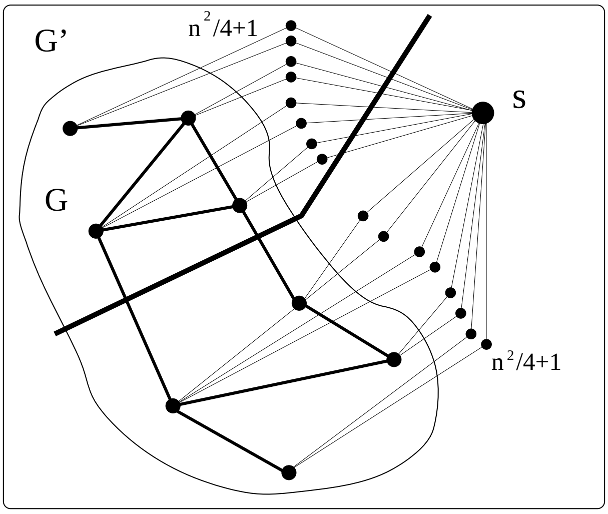

Figure 1: Polynomial reduction of optimal attack to graph bisection

Lemma The original graph G has a bisection of size $B, 1 \leq B \leq |V|^2/4 < |V|^2/4 + 1$ if and only if ($\Longleftrightarrow$) the serverless communication network G' has an attack A with $D_{G'}(A) \geq \frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) + \frac{|V|}{2}$ and $C_{G'}(A) \leq \frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) + B$.
only if ($\Longrightarrow$) If there exists a bisection $B = (V_1, V_2)$ of size lower or equal to B we construct an attack A in the following way, $A = \{(v_1, v_2) \in E \mid v_1 \in V_1 \ and \ v_2 \in V_2\} \cup \{(a^i_{v_j}, s) \in E' - E \mid v_j \in V_1 \ and \ i = 1 \cdots (|V|^2/4) + 1\}$. The cost of this attack

is clearly $C_{G'}(A) \leq \frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) + B$. This attack disconnects $\frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) + \frac{|V|}{2}$ nodes from the connected component of size $\frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) + \frac{|V|}{2} + 1$ that contains the extra node s. As the connected component that contains s has a size bigger that $|V'|/2 = \frac{1}{2}(|V|^3/4 + 2|V| + 1)$ its clear that the connected component that contains s is B_{cc} of graph G'. This means that the damage produced by A is the size of the elements of V' that do not belong to B_{cc} i.e. $\frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) + \frac{|V|}{2}$.

if ($\Longleftarrow$) As $D_{G'}(A) \geq \frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) + \frac{|V|}{2}$ and $|V'| = |V|^3/4 + 2|V| + 1$ then the size of B_{cc} is at most $|V'| - D_{G'}(A) = \frac{|V|^3}{8} + |V| + 1$. This means that any node in the graph G' (and in particular the special node s) must be disconnected from at least $|V'| - |B_{cc}| = \frac{|V|^3}{8} + |V|$ nodes in the graph G'.

Suppose now that the attack disconnects from s a number t of nodes from the original graph G with $t < |V|/2$. As s must be disconnected from t nodes from V this means that it is necessary to cut the $\frac{|V|^2}{4} + 1$ routes through the auxiliary nodes a_v^i from the extra node s to each of the t nodes. This makes necessary to disable $t\left(\frac{|V|^2}{4} + 1\right)$ links that also disconnects $t\left(\frac{|V|^2}{4} + 1\right)$ auxiliary nodes. Now we need also disconnect at least $\frac{|V|^3}{8} + |V| - \left(t\left(\frac{|V|^2}{4} + 1\right) + t\right)$ nodes by disabling at most $\frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) + B - t\left(\frac{|V|^2}{4} + 1\right)$ links.

As it is not possible to disconnect more nodes from the original graph G, the nodes to be disconnected must be auxiliary nodes corresponding to nodes of G that are still in the same connected component of s. We have to disable the links that lie at the both sides of auxiliary nodes with a total cost of $2\left(\left(\frac{|V|^3}{8} + |V|\right) - \left(t\left(\frac{|V|^2}{4} + 1\right) + t\right)\right) = \frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) - t\left(\frac{|V|^2}{4} + 1\right) + \left(\frac{|V|}{2} - t\right)\left(\frac{|V|^2}{4} + 3\right) > \frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) - t\left(\frac{|V|^2}{4} + 1\right) + B$ due to $\frac{|V|}{2} - t \geq 1$, $\left(\frac{|V|^2}{4} + 3\right) > \frac{|V|^2}{4}$ and $\frac{|V|^2}{4} \geq B$. This means that the attack cannot disconnect from s less than $t < |V|/2$ nodes of the original graph G.

Suppose now that $t > |V|/2$ nodes from G are disconnected from s. To disconnect a node that belongs to V from the extra node s it is necessary to disable at least the $|V|^2/4 + 1$ routes through the auxiliary nodes. As $\frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right) + B \leq \left(\frac{|V|}{2} + 1\right)\left(\frac{|V|^2}{4} + 1\right) < t\left(\frac{|V|^2}{4} + 1\right)$ this means that it is not possible to disconnect from s more that $|V|/2$ nodes. It follows that in the previous conditions an attack must disconnect from s exactly $|V|/2$ nodes of the original graph G.

To disconnect the $|V|/2$ nodes from G from s means a budget of $\frac{1}{2}\left(\frac{|V|^3}{4} + |V|\right)$ allowing at most B for the disabling of further links. The disconnection of the $|V|/2$ nodes from G in this way also disconnects the $\frac{1}{2}\frac{|V|^3}{4} + |V|$ auxiliary nodes in the routes from the $|V|/2$ nodes from G to s. This means that a bisection of weight B or less exists in G if we can separate the $\frac{|V|}{2}$ nodes from G that are connected with s from the $\frac{|V|}{2}$ nodes that are not connected with s by disabling at most B edges from G. ■

The previous theorem can also be established in the case of node based attacks, i.e. $s(v) = 1 \ \forall \ v \in V$, $c(v) = 1 \ \forall \ v \in V$ and $c(e) = \infty \ \forall \ e \in E$. In this case B_{cc} again coincides with the biggest connected component of the graph and the relevance of a connected component coincides with its size.

To establish the theorem for node based attacks in a given graph $G = (V, E)$ let us construct a new graph $G' = (V', E')$ by adding a new extra node v_{ij} in the middle of each edge $(v_i, v_j) \in E$, see figure 2.

Now we assign a serverless communication network to the amplified graph G':

- $V' = V \cup \{v_{ij} | (v_i, v_j) \in E\}$
- $E' = \{(v_i, v_{ij}) | v_i \in V \ and \ v_{ij} \in V'\}$
- $c(e) = \infty, c(v) = \infty \ if \ v \in V \ and \ c(v) = 1 \ if \ v \in V' - V$
- $s(v) = 1 \ if \ v \in V'$

The result follows now by simply applying Theorem 1 to G'.

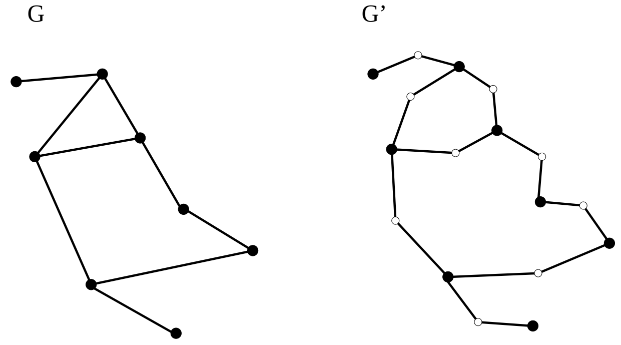

Figure 2: Graph for edges based attacks

4 Approximate algorithms

The previous theorem indicates the necessity of the design of approximate algorithms for the problem of finding optimal attacks. The behavior of random networks and SF networks under approximate attack algorithms based on random selection of the nodes and removal of highly connected nodes is studied by means of computer simulations in [Albert et al. 2000]. In [Holme et al. 2002, Shargel el al. 2003] the "Attack vulnerability" of complex networks to approximate algorithms based on removal of nodes with maximum number of connections and removal of nodes with the highest "betweenness" (i.e. the nodes that appear most frequently in every possible path for each pair of nodes in the graph) is investigated. The "betweenness" is a measure of the centrality of a given node in a network and is exactly calculated as the number of times that the node appears in the shorter paths between the node pairs in the graph. This quantity indicates which are the most important nodes in terms of control of flow of information between pairs of nodes in the network, and their removal would significantly affect to the network connectivity [Newman 2001]. Finding all the node independent paths between a given pair of nodes is a known NP-Complete problems, this fact calls for approximate algorithms to find this quantity, as proposed in [White and Newman 2001] or in [Newman 2005]. The approximate "betweenness" algorithm presents the best results but at the cost of a high computational complexity $O(|V|^4 * |E|)$. Here we study an approximate algorithm based on minimal paths with a lower computational complexity $O(|V|^3)$ that produces similar damage over a set of network models that the "betweenness" algorithm.

We are going to describe the attack algorithms under consideration and calculate the computational complexity of the algorithms.

4.1 Random Failure

This strategy consists of the random removal of nodes that have not been previously removed from the network. The node to be removed is drawn from an uniform distribution and is ca

```
Failure
  j= 1
  n=|V|
  while j < n
    node=aleat(V)
    V = V - node
    j++
End Failure
```

Where V is the set of nodes in the graph, the function $aleat(V)$ returns a node selected at random among the nodes that have not been removed from the network. If we assume that the function $aleat(V)$ has a computational complexity $O(1)$ it is easy to see that the algorithm has complexity $O(|V|)$.

4.2 Degree Based Attack

This strategy is based on the idea that removal of the most connected nodes in terms of their number of neighbors will cause higher damage to the network connectivity.

```
AttackDegree
  j= 1
  n=|V|
  while j < |V|
    node=MostConected(V)
    V = V - node
    j++
End Attack
```

In general an implementation of $MostConected$ will need to cover the list of nodes that has not been previously removed and to count the number of neighbors that each of the nodes has. It is necessary to point out that each time a node is removed, the number of neighbors of other nodes in the graph is modified. The asymptotic behavior of this algorithm is $|V| + (|V| - 1) + (|V| - 2) + \cdots + 1$, where each term in the sum corresponds to a call to the function $MostConected(G)$. This means, adding the previous expression, that the computational complexity of this algorithm is $O(|V|^2)$.

4.3 Minimal Path Based Attack

This method is based on the concept of node "betweeness" [Newman 2001] assuming that the nodes that appear in the highest number of shorter paths between pair would cause the highest damage in terms of connectivity if they are removed.

```
AttackMinPath
  j= 1
  n=|V|
  while j < n
    For each u in V
      ind[u]=0
      For each u,v in V
        C = minimal path from u to v
        for each node k in C
        ind[k]++
        node = k such as ind[k] is maximum
        V = V - node
        j++
End AttackMinPath
```

At each iteration, for the calculation of the minimal path between every pair of nodes in the graph we can perform $|V| - j + 1$ calls to a Dijkstra-like [Cormen et al. 1998] algorithm for the $|V| - j + 1$ nodes that has not been removed from the graph. Given that Dijkstra's algorithm has a complexity $O(|V| + |E|)$ and considering disperse graphs, (in particular we have $|E| \propto |V|$), the execution time of the algorithm is $|V|^2 + (|V| - 1)^2 + \cdots + 1$. This means that our algorithm has a complexity $O(|V|^3)$. In the case of dense graphs, there exist algorithms that calculate exactly a path between every pair of nodes in the graph with a complexity $O(log(|V|)|V|^{2.376})$ [Seidel 1995]. The minimal path based attack algorithm can also be approximated by a statistic method by selecting only a subset of the total set of pairs of nodes in the graph.

5 Network topologies

We are going to study the algorithms presented in the previous section over a set of different topologies. These topologies represent the most usual models of complex networks that are proposed in the bibliography. In particular the models under study are:

5.1 Regular Network

Regular networks are mainly used in analytic studies of the performance of protocols or in the study of the behavior of some metrics. The structure of the regular network makes tractable the study of some problems [Zhang 2000].

5.2 Real Network

The models based on real networks are used for the study of the properties of that particular network. The main problem of these models is that the results are not only limited to that particular network but also the results are only valid for a relatively short period of time due to the fact that most of the real networks grow by augmenting the number of nodes and/or edges or by simply changing its connectivity. In general these networks are used to test that the metrics selected in other types of network coincide with the ones present in real networks. As an example of Real Network, in this work we have selected the publicly available data of the Power grid of the west of United States [Matrixmarket]. This particular real network also present an order, clustering and average path similar to the artificial network models under consideration in this work what makes it suitable for comparison with the artificial topologies.

5.3 Random Network

Random Networks are networks where the connections between nodes are established at random These networks were studied mainly by Erdös and Rényi [Erdös and Rényi 1959] and Bollobas [Bollobas 2001]. These works are based mainly on the fact that most of the properties of the random graphs can be studied analytically by probabilistic methods.

5.4 Transit-Stub Hierarchical Network

Transit-stub hierarchic topologies are presented in [Aguirre et al. 2003]. This topologies represent networks where sets of nodes are connected with the rest of the network by a small number of outputs. These networks resemble most accurately certain networks such as communication networks or the Internet [Zegura et al. 1997].

5.5 Small-World Network

Small-World networks [Watts 1999, Watts and Strogatz 1998] are networks with high local clustering and small distances between the nodes. SW topologies present some very interesting features that make them very suitable for efficient transmission of commodities [Aguirre et al. 2000]. They appear naturally in many real life networks.

5.6 Scale-Free Network

The Scale-Free model [Barabási and Albert 1999] shows a power law distribution of the degrees of the nodes. This model presents a short distance between nodes and a low clustering coefficient.

5.7 Mixed Scale-Free Small-world Network

We also consider a mixed SF-SW model with $n = 2000$ and $< k >= 8$ with high local clustering, small distance between nodes and a power law degree distribution. This mixed model has been built in three steps, first we build a SF graph $G_1 = V, E_1$ following the Barabási and Albert model with parameters $m_0 = m = k/2$ and $t = n - m_0$. Then we build a regular ring lattice $G_2 = (V, E_2)$ with degree $k' = k/2$ that uses the set of nodes generated in G_1. Finally we build the graph $G = G_1 \cup G_2$. This strategy corresponds with the fact presented in [Boudourides and Antypas 2002] where in the evolution process of a communication network, besides the preferential connection scheme presented in the SF networks, each node establishes connection with nodes that present

	L	C	B
RING	125.438	0.643	1
POWER GRID	15.808	0.056	428
RANDOM	3.89	0.004	6
TRANSIT STUB	18.77	0.75	183
SMALL-WORLD	14.2	0.626	1
SCALE-FREE	3.409	0.019	1
MIXED	3.744	0.157	1

Table 1: Values of L and C and B for different graphs models

similar characteristics (geographic, thematic, etc). As can be seen in table 1 this model presents a high clustering and a low path length maintaining a power law distribution of the degree of the nodes.

In this work we will study the following networks:

- Regular topologies: Regular ring-lattice with $|V| = 2000$, $< k >= 8$,
- Real topologies: Power grid of the west of United States $|V| = 1454$, $< k >= 2.66$,
- Random topologies: Erdös and Rényi model random network $|V| = 2000$, $< k >= 8$,
- Hierarchical topologies: Transit-Stub Regular graph $|V| = 2000$, $< k >= 8$,
- Small-World topologies: SW graph obtained from a regular ring-lattice $|V| = 2000$, $< k >= 8$ and $p = .01$,
- Scale-Free topologies: Barabási and Albert model SF graph $|V| = 2000$, $< k >= 8$,
- Mixed Scale-Free Small-world topology $|V| = 2000$, $< k >= 8$,

where $< k >$ is the average number of neighbors of each node in the graph.

In order to measure the connectivity of a given network, the most common parameters are the average path distance L, the cluster coefficient C, number of biconnected components B and the distribution of the nodes degrees $p(k)$. The average path distance is a global parameter that shows how far are the nodes of the graph from each other in terms of their shortest path. The cluster coefficient is a local measure that captures the cliquishness of the neighbors of each node in the graph. Random graphs and SF graphs present a low L and C meanwhile SW graphs present a low L but a high C.

There are some analytical results for the resistance to attacks to some of the previous networks, in particular, the behavior of edge removal in a random network is studied in [Margulis 1974, Bollobas 2001, Cohen et al. 2000]. The Resistance to random attacks in scale free networks is studied in [Albert et al. 2002]. For the study of the resistance of networks attacks we have used an approach similar to the one followed in [Albert et al. 2000] and [Holme et al. 2002]. In our work we have simulated in a computer the behavior of different attack strategies for most network topologies. This approach allows the comparison of the behavior of different attacks strategies and networks topologies under a common framework.

6 Results

In Figures 3 and 4 the behavior of the different models when we use different attack algorithms is depicted. Each value of the x axis is an attack that is determined by its cost. The y axis represent the resistance of the network to that attack.

In Figure 3 it is possible to see that the SW-SF mixed topology shows itself as the most resistant topology when random failures are considered. The SW topology presents the highest resistance to attacks based on the removal of highly connected nodes. When shortest path based attacks are considered, the best results are presented by graphs with random distribution of its connection pattern. Hierarchical networks yield the worst general resistance to attacks. This is due to the high number of articulation points present in this kind of network. Hierarchical is the artificial model that demonstrates a behavior that corresponds most accurately with the results presented by the power grid of the west of the United States.

On the other hand, the attacks based on maximal node degree are not the ones that produce the highest damage in SF networks. As it is shown in Figure 4, for the same given cost, the algorithm based on shortest paths produces a higher damage in all the considered topologies when compared with the attacks based on maximal degree. The attack based on shortest path presents a similar efficiency when compared with the algorithms studied in [Holme et al. 2002]. It can be seen that in all the considered models there exist a rapid change in the behavior of the resistance. That is, there exists a value C_h such as $C > C_h$ $R(A) \sim 0$. In tables 2 and 3 the values $f_{0.01} = min\{C(A)/R(A) < 0.01\}$ and the average value of $R(A)$ are shown for the different attack strategies over the considered network models. This change of behavior can be utilized as another measure of the efficiency of the algorithm.

In table 4 it is shown that the algorithm based on shortest paths presents the best efficiency in every kind of network. The worst efficiency for the three types of algorithms are obtained in the random and mixed topologies.

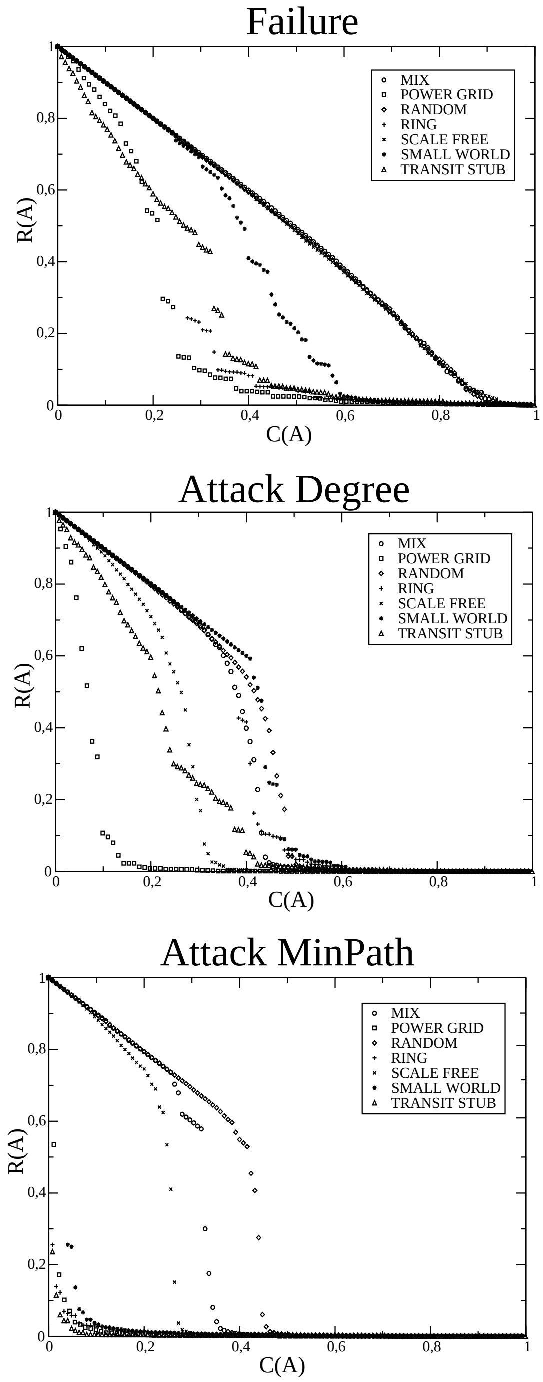

Figure 3: Graphs resistance for different attack strategies.

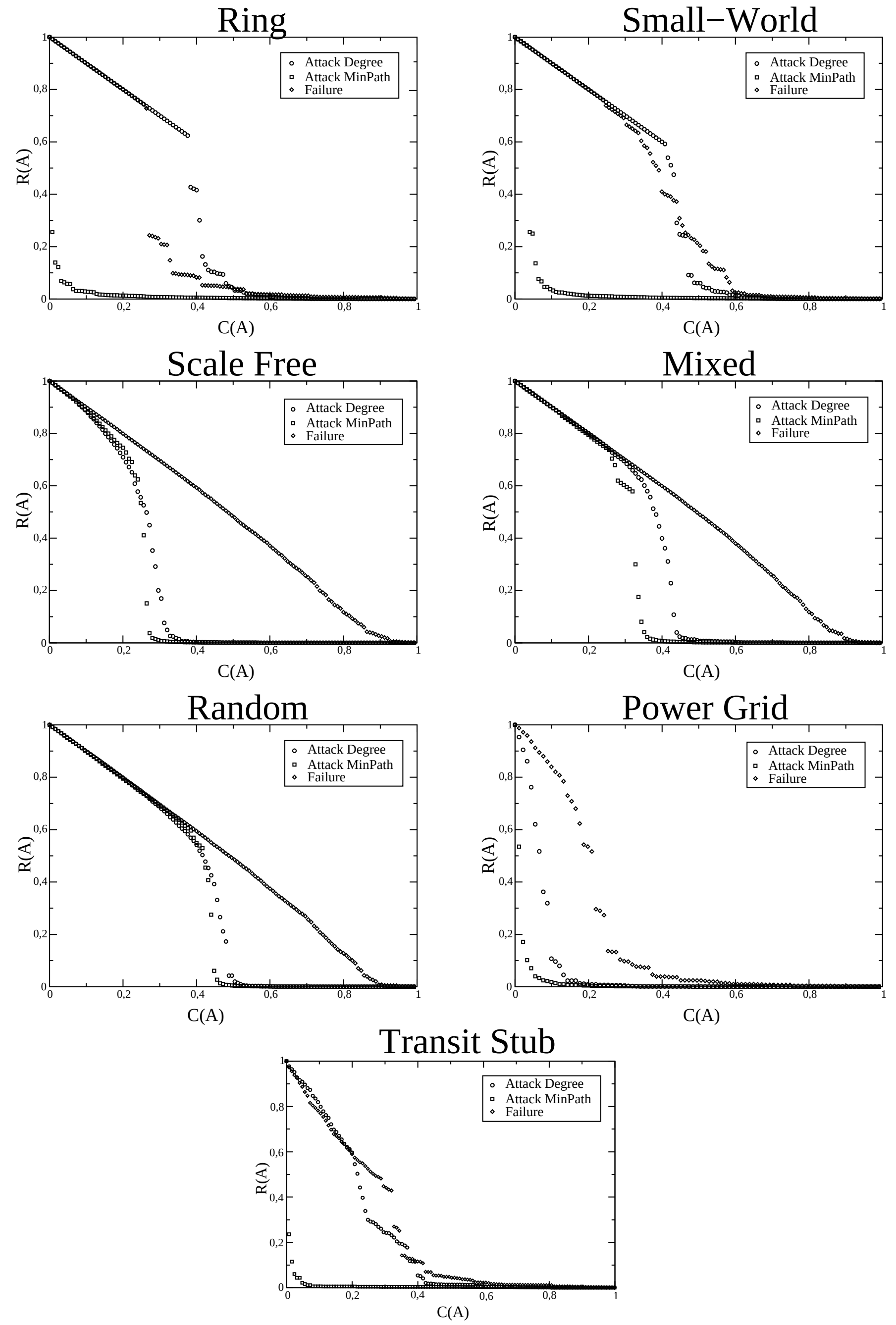

Figure 4: Resistance to attacks for different kinds of graphs.

	Failure	Degree	Min path
RING	0.26	0.33	0.02
POWER GRID	0.20	0.07	0.02
RANDOM	0.47	0.35	0.34
TRANSIT STUB	0.25	0.22	0.01
SMALL-WORLD	0.36	0.35	0.05
SCALE FREE	0.47	0.23	0.22
MIXED	0.48	0.32	0.27

Table 2: Average value of the network resistance to different attack strategies.

	Failure	Degree	Min path
RING	0.71	0.60	0.26
POWER GRID	0.66	0.19	0.13
RANDOM	0.89	0.52	0.47
TRANSIT STUB	0.81	0.57	0.07
SMALL-WORLD	0.70	0.61	0.27
SCALE FREE	0.93	0.35	0.30
MIXED	0.91	0.49	0.39

Table 3: Value of $f_{0.01}$ for different attack strategies.

7 Summary, conclusions and future work

In this paper we have investigated the complexity of the problem of optimal attack to a serverless network. We have provided the necessary definitions and stated that the problem is NP-Complete even in the case when only edges or nodes can be removed. We have constructed an auxiliary graph in order to show that there exists a polynomial reduction of this problem to the minimal bisection

	Failure	Degree	Min path
RING	1.50	1.29	4.87
POWER GRID	1.80	2.88	4.23
RANDOM	1.03	1.25	1.28
TRANSIT STUB	1.77	1.81	5.28
SMALL-WORLD	1.24	1.24	3.21
SCALE FREE	1.04	1.62	1.66
MIXED	1.03	1.31	1.45

Table 4: Average value of the efficiency for different attack strategies.

problem. We have also studied an approximate algorithm with a computational complexity of order $O(|V|^3)$ based on minimal paths that outperforms algorithms based on random failures or maximal node degree. This algorithm presents similar efficiency when compared with algorithms of higher computational complexity. With the increasing relevance of P2P networks more and most powerful approximate attack methods, and attack resistance topologies are needed, some very interesting works are appearing last years [Li 2004, Li 2006], but a further effort is needed to develop new techniques suitable to not centralized networks. These methods also could allow variable cost and damage functions instead of *a priori* fixed values.

References

[Abdelouahab et al. 2009] Abdelouahab M. A., Bouabdallah A., Achemlal M., Laniepce S., "The topology change attack: threat and impact", Journal of Universal computer Science, Vol. 15, No. 2, (2009), 465–487.

[Aguirre et al. 2000] Aguirre C. et al. "Small-world topology for multi-agent collaboration". Proceedings 11th International Workshop on Database and Expert Systems Applications, London, IEEE Comput. Soc (2000), 231–235.

[Aguirre et al. 2003] Aguirre C., Corbacho F. and Huerta R., "Static and Dynamic properties of Small-World connection topologies based on Transit-stub Networks", Complex Sytems 14, 1 1–28 (2003), 1–28

[Albert et al. 2002] Albert R., Jeong H. and Barabási A.L., "Statistical mechanics of complex networks", Reviews of Modern Physics 74, 47 (2002).

[Albert et al. 2000] Albert R., Jeong H. and Barabási A.L., "Error and attack tolerance of complex networks", Nature 406 (2000), 378–381.

[Barabási and Albert 1999] Barabási A. L. and Albert R., "Emergence of Scaling in Random Networks", Science 286 (1999), 509–511.

[Bollobas 2001] Bollobas B., "Random Graphs, Second Edition", Cambridge University Press (2001).

[Boudourides and Antypas 2002] Boudourides M. A. and Antypas G. P., "A Simulation of the Structure of the World Wide Web", Sociological Research Online (2002).

[Cohen et al. 2000] Cohen, R., Erez K., ben-Avraham D. and Havlin S., "Resilience of the Internet to random breakdowns", Physical Review Letters 85, 4626 (2000).

[Cormen et al. 1998] Cormen T. H. et al., "Introduction to algorithms", The MIT Press (1998).

[Cunningham 1985] Cunningham W. H., "Optimal attack and reinforcement of a network", Journal ACM 32(3) (1985), 549–561.

[Erdös and Rényi 1959] Erdös P. and Rényi A., "On Random Graphs I.", Publ Math. Debrecen 6 (1959), 290–297.

[Fortz 2000] Fortz B., "Design of Survivable Networks with Bounded Rings (Network Theory and Applications)", Kluwer Academic Publishers (2000).

[Garey and Johnson 1976] Garey M. R. and Johnson D. S., "Some simplified NP-Complete graph problems", Theoretical Computer Science 1(3) (1976), 237–267.

[Grover 2003] Grover W. D., "Mesh-based Survivable Networks", Prentice Hall (2003).

[Holme et al. 2002] Holme P. et al., Attack vulnerability of complex networks", Physical Review E 65 05609 (2002), 1–13.

[Koukopulos 2009] Koukopoulos D., "Stability in heterogeneous multimedia networks under adversarial attacks", Journal of Universal computer Science, Vol. 15, No. 2, (2009), 444–464.

[Leiwo et al. 2000] Leiwo J., Nikander P., Aura T., " Towards network denial of service resistant protocols", Proc. Sixteenth Annual Working Conference on Information Security (SEC2000) IFIP Series, Vol. 175, (2000)

[Li 2006] Li, M., "Change trend of averaged Hurst parameter of traffic under DDOS flood attacks", Computers & Security, Vol. 25, No. 3, (2006), 213–220.

[Li 2004] Li, M., "An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition", Computers & Security, Vol. 23, No. 7, (2004), 549–558.

[Margulis 1974] Margulis, G. A., "Probabilistic characteristics of graphs with large connectivity", Problems of Information Transmission 10 (1974), 174–179.

[Matrixmarket] www.matrixmarket.com or gams.nist.gov/MatrixMarket

[Newman 2001] Newman, M. E. J., "Scientific collaboration networks: II. Shortest paths, weighted networks, and centrality", Phys. Rev. E 64, 016132 (2001).

[Newman 2005] Newman, M. E. J., "A measure of betweenness centrality based on random walks", Social Networks 27 (2005) 3954.

[Seidel 1995] Seidel R., "On the All-Pairs-Shortest-Path Problem in Unweighted Undirected Graphs", Journal of computer and system sciences 51 (1995), 400–403.

[Shargel el al. 2003] Shargel B., Sayama H., Epstein I. R. and Bar-Yam Y., "Optimization of Robustness and Connectivity in Complex Networks", Physical Review Letters 90(6) 068701 (2003).

[Stoer and Wagner 1997] Stoer M. and Wagner F., "A simple min-cut algorithm", Journal ACM 44(4) (1997), 585–591.

[Watts 1999] Watts D. J., "Small Worlds: The dynamic of Networks between Order and Randomness", Princeton University Press (1999).

[Watts and Strogatz 1998] Watts D. J. and Strogatz S. H., "Collective dynamics of small-world networks", Nature 393 440 (1998).

[White and Newman 2001] White R., Newman M. E. J. ,"Fast Approximation Algorithms for Finding Node-Independent Paths in Networks", Santa Fe Institute working papers 7035 (2001).

[Zegura et al. 1997] Zegura E. W., Calvert K. L. and Donahoo M. J., "A Quantitative Comparison of Graph-Based Models for Internet Topology", IEEE/ACM Transactions on Networking 5(6) (1997).

[Zhang 2000] Zhang L., "Fault tolerant networks with small degree", Proc. 11th ACM symposium on Parallel Algorithms and Architectures (2000).