Federal University of Paraná

Department of Informatics

Robson Melo, Aldri Santos, Michele Nogueira, Deep Medhi[1]

Resilience and Knowledge in a Metric for Heterogeneous Wireless Connectivity

Technical Report
RT-DINF 003/2013

Curitiba, PR
2013

[1]Curators' Professor, Computer Science & Electrical Engineering Department, University of Missouri-Kansas City, USA.

Abstract

Complex networks' metrics and minimum cut trees have been used in different network contexts in order to describe and learn from the Internet and Web structure, or to identify the maximum flow capacity in routes. In wireless networks, user nodes' mobility, cryptographic key management, and network connectivity have been characterized using complex networks models. In the past, the use of complex network models in telecommunications has not been extensively considered to analyze resilience in networks. However, nowadays, with the increasing computation capacity of modern devices, complex networks and minimum cut trees may be employed to identify or predict failures. In this paper, we present *connectivity antifragility*, a new network measure that quantifies the impact of each node or failure in network connectivity and provides knowledge to the network learn from failures and redesign connections online. Moreover, this measure allows the identification of a set of more vulnerable connections under failures. In addition, two applications of this measure are presented, considering real traces from heterogeneous wireless networks available at the CRAWDAD web repository and from a cellular network. Results show that connectivity antifragility can assist in identifying the most vulnerable connections in the network and quantify them.

1 Introdution

In the last few years, complex networks have been applied to different areas such as sociology, biology, physics and computer science in order to understand the characteristics of non-uniformly random connectivity in real world networks. Complex networks techniques have assisted to discover the scale-free structure in the Internet and in the WWW. Similarly, the minimum cut tree techniques, such as Gomory-hu, have been successfully employed to support clustering and maximum flow analyses. In wireless context, complex networks have assisted to analyze the behavior of machine-to-machine (M2M) communication, cellular, sensor and ad hoc networks. However, these techniques have never been employed extensively in telecommunications to analyze resilience. When applied, they have considered independent failures only as avoidable events without taking into account the characteristics and requirements resulted from the simultaneous use of different technologies and networks.

People have depended on technology to assist them perform work along the last few years. Technology has evolved from very simple ideas, and since the industrial revolution it has become increasingly ubiquitous. Further, wireless communication has been more widespread, assisting different sectors of Society, as healthcare, aeronautics, commerce, transportation and others, with wireless network-based systems, and systems of these systems resulting in emergent behaviors from technology convergence. As wireless networks continue to increase in scale and complexity, new approaches are required to describe emergent behaviors and learn from them.

However, the convergence of different communication technologies brings issues, mainly over *availability* aspect. Vulnerabilities initially restricted to a single type of network may proliferate to others by the integration of convergent heterogeneous environments [Ghosh et al. 2012]. Security strategies, conceived for only one type of network, are ineffective and require a redesign in case of a convergent context [Hashim et al. 2012]. Also, convergence can result in previsouly inexistent security issues and failures, that can directly or indirectly compromise the availability of services in the network. In addition, the nomadic profile of mobile devices contributes to virus, malware, and other vulnerabilities propagation affecting other users and the network as a whole.

Proposals ensuring resilience to network are fundamental in order to tolerate the frequent disconnections of mobile terminals and reduce availability issues [Sterbenza et al. 2010, Ackley 2013]. Resilience enables a network to survive and stand from failure. In the literature, algorithms and metrics have been proposed to identify rare events and analyze resilience in homogeneous

wireless networks connectivity [Sterbenza et al. 2010, Heegaard and Trivedi 2009, Qin et al. 2013]. In [Qin et al. 2013], for instance, authors proposed a metric referred to as node criticality index that could be employed to predict failures, making the network stronger. Also, proposed approaches evaluate the impact of failures in data flows of heterogeneous networks. However, they do not evaluate connectivity robustness or fragility in connectivity of heterogeneous wireless networks. Neither, they consider successive failures or disturbance as a source of knowledge to improve on the fly network resilience.

In this paper, we present *connectivity antifragility*, a new network measure that describes the impact of each node or failures in network connectivity, providing knowledge to learn from them and redesign network connections on real time. Taking advantage of the increasing computation capacity in modern mobile devices, this measure allows to identify the most vulnerable connections under failures or other disturbances on heterogeneous wireless networks based on powerful techniques of complex networks and graph theory. This metric assesses the connection fragility and quantify a set of connections that, if removed, can disconnect all the network. It also quantifies network robustness and indicates alternative connections in order to maintain for longer the network resilience. Two case studies of this measure are provided, considering real traces from heterogeneous wireless networks available at the CRAWDAD web repository and from a real cellular network.

This paper proceeds as follows. Section 2 presents related works. Section 3 describes the system. Section 4 presents the proposed *connectivity antifragility* metric. Sections 5 and 6 illustrate the application of the new metric over heterogeneous mesh networks and celular networks. Finally, Section 7 concludes the paper.

2 Related Work

Works in the literature have identified the necessity of improving network resilience in order to tolerate frequent disconnections of mobile terminals and reduce availability issues on connectivity provided by different technologies of communication together [Zhang et al. 2008]. In [Gardner et al. 2013], the authors introduce a self-pruning algorithm for the identification of rare events and resilience analysis. The algorithm applies characteristics of the network (based on the impact of previous events), and the authors present a metric to measure the impact of rare events in network resilience.

In [Qin et al. 2013], the authors address the impact of failures and QoS changes in heterogeneous networks. They argue that few alterations in a specific network type can affect the traffic flow in all heterogeneous networks,

decreasing the QoS. Their objective was to provide techniques for reliability and resilience in Instrumented Cyber Physical Spaces. Middleware and the reflective methodology OAA (observe–analyze–adapt) were proposed. Based on them, the authors proposed a metric *Node Criticality Index*. However, they did not evaluate connectivity.

In [Cetinkaya et al. 2013], the authors assessed the robustness of multilevel flows on networks. They argue that understanding the Internet evolution from a multilevel perspective is more realistic than examine its properties at individual levels. The authors evaluated real data communication networks and the results showed difficulties caused by partitions on the Internet Service Providers' connectivity (level 1) due to attacks on the logical links. However, robustness evaluation did not consider any attack on the network periphery.

In [Zhang and Sundaram 2012], the authors evaluated network robustness using complex networks. They considered minimum vertice degree as the main metric for robustness. Based on this metric, the authors discussed the difficulty of detecting malicious nodes that broadcast information. The analytical modeling was founded on Erdos-Rényi random graphs, and the results showed that the consensus about the presence of malicious nodes can be achieved in a resilient way without requiring global information. In [Manzano et al. 2013], the authors presented the epidemic survivability metric in order to describe the vulnerability of each node of homogeneous networks under a specific epidemic intensity. The authors showed that the metric can identify the set of nodes that are more vulnerable under an epidemic attack by two case studies.

In [Venmani et al. 2013], the authors presented a metric called *shareability* that measures the ability to share bandwidth. They proposed the *openroutes* framework for failures restoration and disconnections minimization. They also proposed a *cost-effectively* scheme in which two mobile network operators share their resources in order to support the network. The approach employs three heuristic algorithms: the Least Length Shortest Path, Least Delay Shortest Path and Ant Colony Optimization to find the shortest path from the alternative paths available outside of the backhaul. Analyses were perfomed over data from the Sprint U.S. telecommunication network.

Different from these previously mentioned works, in [Barrere et al. 2012], the authors assessed distributed vulnerabilities focusing on autonomic networks and systems. Their main proposal lies in identifying distributed vulnerabilities in order to increase awareness in self-governed environments. Our work contributes with this perspective presenting the connectivity antifragility metric in which we provide information to the network to be able to predict connectivity failures and adapt itself to avoid them.

3 System Description

Consider a topology connectivity of a heterogeneous wireless network modeled by undirected graph $G = (V_G, E_G)$ in which V_G comprises a finite set of vertices that represents network devices (nodes), and where E_G is a finite set of edges that indicates the connections (links) between pairs of devices. Given an edge $e = \{u, v\} \in E_G$, it is said to be incident on u and $v \in V_G$. A connection between two given nodes u and v corresponds also to the connection between v and u, allowing communication in both directions.

Due to the dynamic nature of heterogeneous wireless networks that results from the devices' mobility, or from the use of different technologies, G regards to a discrete instant t. Therefore, at each t, there is a connectivity graph for the network. A sequence of distinct vertices and edges $P = (v_i, e_i, v_{i+1}, e_{i+1}, ..., e_{k-1}, v_k)$ is called the path between v_i and v_k, if $v_i, v_{i+1}, ..., v_k \in V_G, e_i, e_{i+1}, ..., e_{k-1} \in E_G$ and $e_i = \{v_i, v_{i+1}\}$, for $i = 1, 2, ..., k-1$. A path between any u and $v \in V_G$ is called P_v^u. The distance between the two vertices u and v is denoted by $d(u, v)$ and lies in the number of edges that exists between two vertices. The *minimum path* indicates a path of *minimum distance*. Thus, a graph G is called *connected*, if for each $u, v \in V_G$ a P_v^u exists. A subset of vertices $X \subseteq V_G$ is a connected component of G, if for each $u, v \in X$, a P_v^u in G exists and X is the maximum subset of vertices. Hence, a network is said to be connected at the instant t, if there is a path for any pair of vertices in G.

A cut C_G of the graph G represents a bipartition of V_G, i.e., a pair of subsets $\{X, Y\}$ such that $X, Y \neq \emptyset$, $X \cap Y = \emptyset$ and $X \cup Y = V_G$. This cut represents possible connectivity failures in links on the network. The cut size lies in the number of critical links that, if removed, should disconnect the network. The *minimum cut* (*mincut*) indicates the lowest cut size, i.e., the minimum number of critical link failures resulting in a network disconnection. Therefore, being $u, v \in V_G$, a cut_v^u of G is a cut in the sets $\{X, Y\}$ in which $u \in X$ and $v \in Y$. A $mincut_v^u$ is a cut_v^u of minimum distance. Furthermore, local edge-connectivity between u and v in G, denoted by $\lambda G(u, v)$, means the distance of a *mincut*. Identifying the *minimum cut* in a specific path assists in pointing out vulnerable links in a path and in the network. A *cut tree* T_c of G consists in a tree such that, for each $u, v \in V_G$, the cut induced by removing the minimum capacity edges in P_v^u in T_c is a $mincut_v^u$ of G.

4 Defining Antifragility Metric

In this section, we present our new network measure called *connectivity antifragility* (CA). We define our proposal as the level of avoiding criticality in connections of a network under disruptions. By criticality, we consider the probability a network disconnection that can result from disruptions, caused by attacks, accidents, or failures. Our main goal lies in providing knowledge to assist the network to learn from its damaging conditions or to be prepared to deal with them. We founded our metric on the antifragility concept that goes beyond resilience and robustness and promotes self-learning and self-adaptation of the network, when enduring failures, in order to apply cost-effectively mechanisms that are able to address them [Tseitlin 2013].

We employ *minimum cut tree* and *clustering* techniques. Based on these techniques, the connectivity antifragility metric is designed to identify the most vulnerable connections and quantify the robustness in the network. The two techniques provide information composing the connectivity antifragility metric. This metric offers knowledge to the network, then it can autonomously learn, change, and predict connection conditions. If applied partially, the metric can identify the most fragile connections using *Gomory-Hu*, a minimum cut tree algorithm, and it can also assess the correlation among the devices. In the next subsections, we present two partial and complementary measures respectively calculated based on the mimimum cut tree algorithm and the cluestering coefficient. We correlate them these two measures into the CA metric.

4.1 Gomory-Hu tree

A *Gomory-Hu* tree consists in a weighted tree $T_c = (V_T, E_T)$. Weights in T_c correspond to all $mincut_v^u$ between the pairs of vertices $u, v \in V_T$, being $V_T \equiv V_G$, given a graph $G = (V_G, E_G)$ and representing a network topology at an instant t. The minimum cut tree T_c for a heterogeneous network G results from the following procedure. Given G, for each pair of nodes $u, v \in V_G$, the $mincut_v^u$ is identified by the minimum $d(u, v)$, corresponding to the lowest number of connections that, if under disruption, can disconnect the network. Based on the minimum $d(u, v)$, G is separated into two components (new graphs) X, Y, where $u \in X$ and $v \in Y$. This procedure repeats recursively for each resulted component until X and Y own a unique node. In our application of the algorithm, it provides the outcomes T_c and a set W_c of T_c weights.

Figs. 1 and 2 illustrate a graph G representing a network topology and a Gomory-Hu tree extracted from G. In Fig. 2, weights represent how many

edges between the indicated vertices are necessary to disconnect G. For instance, in T_c, the highlighted dashed edge between vertices 4 and 101 owns a weight of value 6, meaning that if 6 edges in the paths between vertices 4 and 101 are removed, the network is disconnected. This logic is employed for the different edges in T_c.

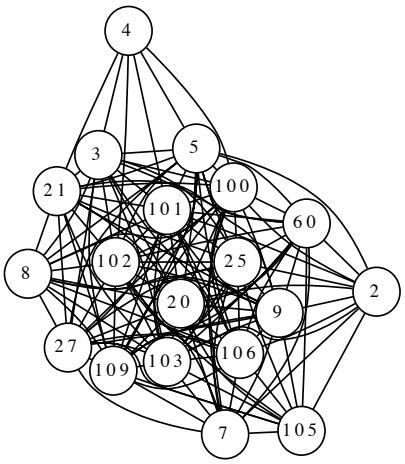

Figure 1: A graph G for a network topology

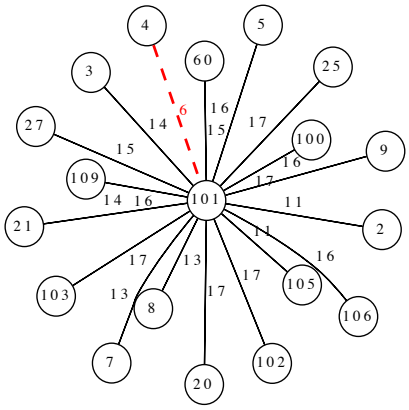

Figure 2: Gomory-Hu tree for G

From the mimimum cut tree T_c and the set W_c, we calculate a partial measure called network fragility (NF). Following the concept that it never pays to make any link of a *chain* stronger than the weakest link [J. and M'Raïhi 1999], the network fragility is calculated by the ratio between the minimum weight and the maximum weight in T_c among all the weights of E_T. Eq. 1 represents the NF calculation.

$$NF = \frac{min\{w|\forall w \in W_c\}}{max\{w|\forall w \in W_c\}} \tag{1}$$

In order to illustrate this, we take Fig. 2 as example to represent the minimum cut tree T_c for a network topology modeled by a graph G. Among all the edges of T_c, the minimum weight is 6 and the maximum is 17. Hence, the NF for this network is approximately 0.35, meaning that the level of fragility for this network is 35%. Also, taking this figure as example, we highlight that the minimum cut involves six different edges in the network topology represented by G. These six edges, called critical links, are in the paths between 4 and 101, as shown in Fig. 19 by dashed lines. Similarly, we call critical vertices as those connected by critical links. In the figure, critical vertices are 3, 4, 5, 21, 100, 101, and 102.

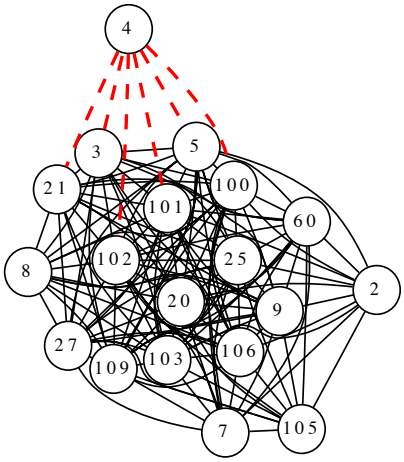

Figure 3: Critical links highlighted by dashed lines

4.2 Clustering coefficient

Another important aspect that can compromise connectivity in networks is transitivity or vertices' relationships, particularly, critical vertices. Given a vertex v directly connected to another u, these vertices are considered neighbors. The degree of v corresponds to the sum of its neighbors, denoted by d_v. The clustering coefficient of $v \in V_G$ implies the amount of edges that the neighbors of v have between them, divided by the total amount of edges v could have.

Through d_v, we can also indicate the largest number of edges that v can have given by $B = \binom{d_v}{2}$. Being E_v the real number of edges that v has, i.e., its current number of neighbors, it is possible to define the clustering coefficient of v, C_v, as shown by Eq. 2. In our context, the clustering coefficient indicates the level of redundancy that a node can have in terms of connections. This measure is also the number of cliques, size 3, in a graph.

$$C_v = \frac{E_v}{B} = \frac{2 \cdot E_v}{d_v \cdot (d_v - 1)} \tag{2}$$

The clustering coefficient of the vertices can be employed to calculate a global clustering coefficient (C_{Global}) to the network as the lowest C_v among all vertices in G, as shown in Eq. 3

$$C_{Global} = min\{C_v | \forall v \in V_G\} \tag{3}$$

Based on these definitions, we calculate another partial measure called fragility degree (FD), given by Eq. 4. We also follow the concept that it

is most important to focus on the weakest links and vertices of a network. Hence, we take (as reference) the set of critical vertices (CV), composed of all vertices in the paths related to the lowest $mincut_v^u$ of T_c. We calculate C_v for all those vertices. Then, FD lies in the ratio between the minimum and the maximum C_v calculated.

$$FD = \frac{min\{C_v|\forall v \in CV\}}{max\{C_v|\forall v \in CV\}} \tag{4}$$

As an example, for a network represented by G, Fig. 4 and 5 respectively show the clustering coefficient for each vertex and the value global clustering coefficient C_{Global} 0.82, indicated in vertices with a bold border.

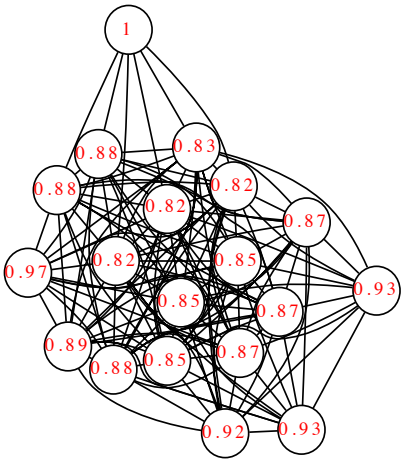

Figure 4: Clustering coefficients for each vertice

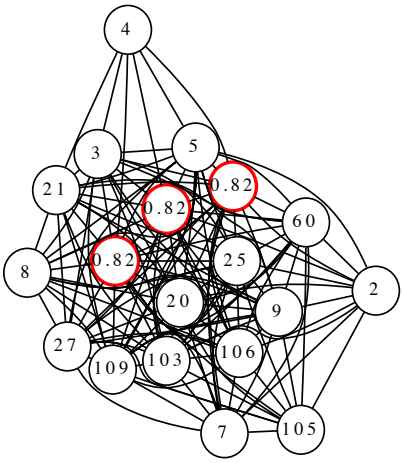

Figure 5: Global clustering coefficient

4.3 Correlating minimum cut and clustering coefficient into the antifragility metric

The partial measures NF and FD obtained by Gomory-hu and clustering coefficient techniques are complementary since the first one indicates and quantifies the most vulnerable connections in the network by T_c and W_c, and the second one calculates the fragility in the neighborhood of the most vulnerable vertices. The quantification and location of critical links, that (if removed) can disconnect the network is fundamental to the development of countermeasures for prevention and resilience to failures in connectivity. In order to take advantage of these two kinds of knowledge, we propose a connectivity antifragility metric defined by Eq. 5.

$$CA = 1 - (\alpha \times NF + \beta \times FD) \quad (5)$$

The constants α and β represent the importance given to NF or FD. Since NF is the starting point for all posterior analyses, we consider that NF has a greater impact on calculating the level of antifragility in connections. NF indicates the most vulnerable connections of the network, and based on that connection, redundancies (provided by vertices) neighbors can be calculated. Hence, we believe that α tends to always have greater values than β. However, $\alpha + \beta = 1$.

5 Case study 1: Antifragility over heterogeneous mesh networks

We show the application of the connectivity antifragility metric on a heterogeneous wireless network as case study 1. We employ it over real traces from the *MeshNet*[1] project performed in 2007 at the University of California in Santa Barbara (UCSB) and available on the CRAWDAD web repository[2]. Next, we detail the methodology and numeric results. The network of the *MeshNet* project is comprised of 19 mesh nodes operating in two different standards, *802.11a/b*, creating a heterogeneous network in terms of a communication pattern. A set of 900 files composes the traces, each one representing different instants t with various connectivity conditions and network topology. We have filtered the files in order to identify instants in which the network was fully connected, resulting in 577 files. Each line of the traces determines a connection between nodes. The first column of the trace consists in the *IP* address of a specific node, followed by columns containing *IP* addresses of each node connected to it.

A graph was created for each trace file, representing a graph for each instant t. Fig. 1 also gives an example of a graph for a specific instant t for this network. Over these graphs, we have applied the *Gomory-Hu* algorithm, and we have calculated the *clustering coefficient*. Also, we calculated the value of NF, FD, and CA metrics for each one. For the *Gomory-Hu* algorithm application, we have employed the implementation provided by the LEMON[3] library. A Python *script* was implemented to automatically filter the trace files and process the graphs. The application of the *Gomory-Hu* algorithm identifies the lowest cut_v^u for each graph and the critical vertices.

[1] http://moment.cs.ucsb.edu/meshnet/

[2] http://crawdad.cs.dartmouth.edu/meta.php?name=ucsb/meshnet

[3] http://lemon.cs.elte.hu/trac/lemon

In our analysis, we considered *high fragility* as the network topology that presents a lower number of links to disconnect it. *Low fragility* means a high the number of links to disconnect it. We also calculate the *clustering coefficient* to identify the relationships between the neighbors of a given vertex and determine its connectivity robustness.

5.1 Results

Fig. 6 presents the results for the connectivity antifragility metric over heterogeneous mesh networks with a variation in α and β values. As explained, NF indicates the level of network fragility from the most vulnerable network connections. Hence, we consider that this measure has a greater impact on the calculation of the antifragility level. Thus, we performed a variation of the weights assigned to NF and FD, in which values for α are always higher than β. For $\alpha = 0.6$ and $\beta = 0.4$, CA ranges from 0.4 and 0.5 observed during all instances. For $\alpha = 0.9$ and $\beta = 0.1$, we observe an oscillation during all instants, however CA ranges from 0.5 to 0.6. From the results, we observe that the values of α and β have a strong influence on the CA result.

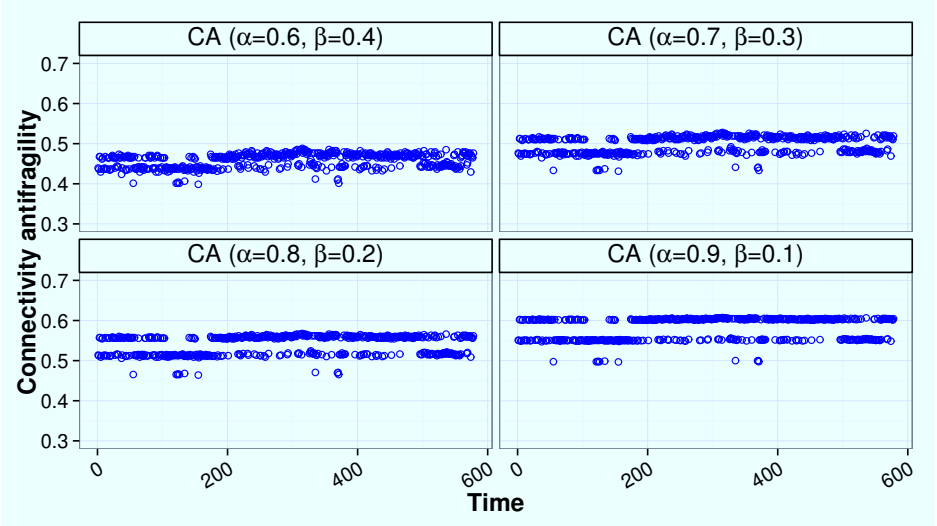

Figure 6: Connectivity antifragility for heterogeneous mesh network

Fig. 7 shows the values of NF and FD measures for the 577 different instants of time for the network. We label time varying from 0 to 600 unities of time. NF values range from 0.3 to 0.45, which correspond to a fragility index between 30% and 45% over the network connectivity. FD values for all instants of network operation range between 0.75 and 0.85. These re-

sults indicate that critical vertices present a high relationship among their neighbors.

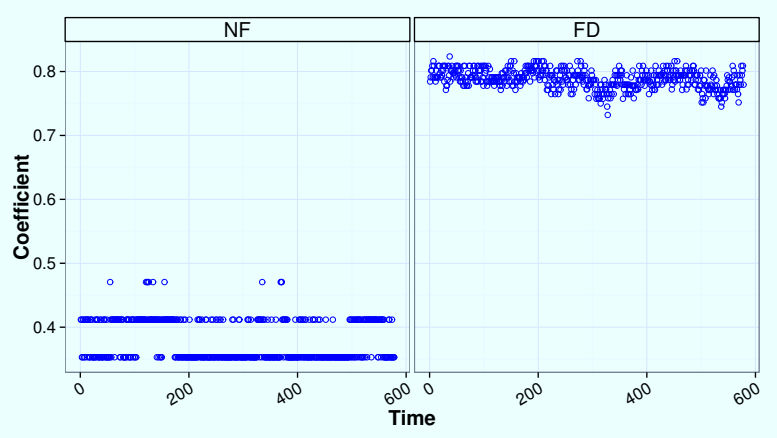

Figure 7: Analyzing NF and FD on different instants of the network

Fig. 8 represents the variations (mean and confidence interval) of the number of neighbors for each node during all instants t. It shows network dynamics. In the figure, we present a minimum, average, and maximum number of neighbors for each node for each instant. Node 25 has the highest number of neighbors and node 4 the smallest one, considering analyses for a given instant of the network. Fig. 9 shows the frequency of the three minimum cut sizes in the network to every t.

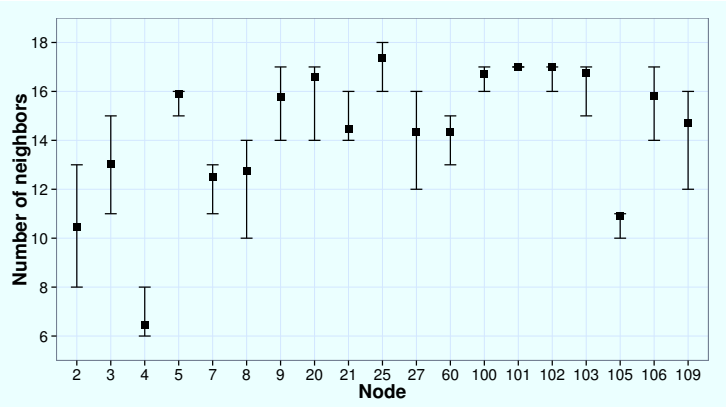

Figure 8: Node degree variation at all instants

The network is dynamic, making it difficult to guarantee connectivity at all times. However, in this case study, there is certain stability for the

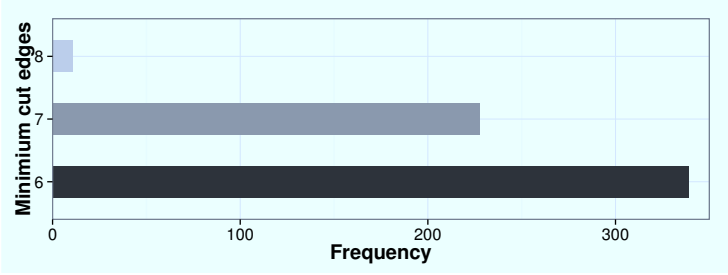

Figure 9: Frequency of the minimum cut sizes

values of minimum cut size, ranging from 6 to 8. Another point identified by the results is the existence of specifics links constantly appearing in different groups of links with *higher fragility*. This indicates that these links are regularly indicated as the weakest ones in the network, as shown in Fig. 10, set A. Table 1 correlates edges and sets, and Fig. 10 shows that the edges belonging to the set A show up repetitively between the links of higher fragility.

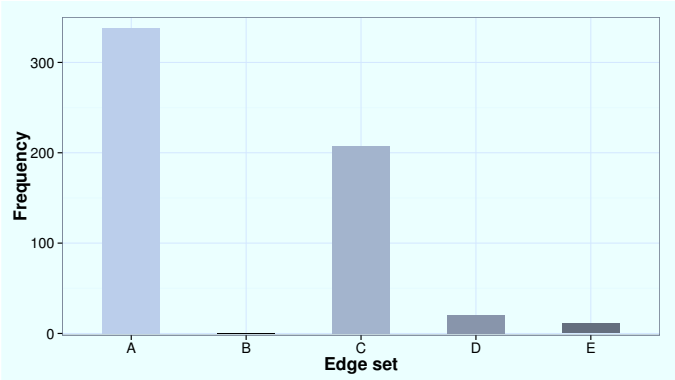

Figure 10: Set of fragile edges

Table 1: Set of the most vulnerable edges

Sets	**Edges**							
A	4, 101	3, 4	4, 100	4, 5	4, 21	4, 102	-	-
B	4, 101	3, 4	4, 100	4, 5	4, 21	4, 25	-	-
C	4, 101	3, 4	4, 100	4, 5	4, 21	4, 25	4, 102	-
D	4, 101	4, 8	3, 4	4, 100	4, 5	4, 21	4, 102	-
E	4, 101	4, 8	3, 4	4, 100	4, 5	4, 21	4, 25	4, 102

In order to evaluate the robustness in critical vertices' connections in the network, the *clustering coefficient* is presented. The cluster establishes a

number of connections between the neighbors of a node. These connections can define the number of alternative paths. For each instant t, we calculate clustering coefficients for each vertex and also for the network. After the individual instant analyses, the evaluation for the entire period is performed in order to find the variation of the clustering coefficients and global clustering coefficient.

Fig. 11 shows C_v variation (mean, median, quartiles) for each node along all 577 instants. The vertex 4 keeps its rate constant for C_4 during every moment of network observation and with a value equal to 1.0, indicating the existence of different links between its neighbors, that provide alternative ways to reach them.

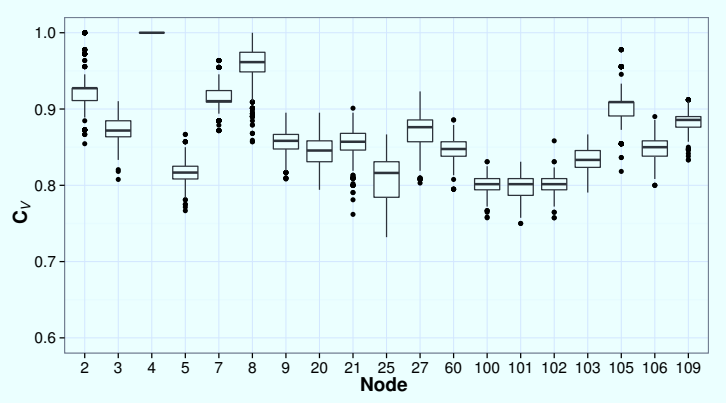

Figure 11: Clustering coefficient variation

Fig. 12 shows the C_{Global} variation for the network. From the results, we identify a small variation in the rates of the network clustering coefficient, ranging from 0.65 to 0.85. The point highlighted in the figure indicates the instant used in the examples presented in the analysis of clustering coefficients and minimum cut size.

Analyses also help to identify which nodes have a clustering coefficient with the same value as the C_{Global} of the network. In the results, we observed that nodes owning identifiers 25, 100, 101 and 102 presented clustering coefficients as the same value as the C_{Global}. Fig. 13 shows the frequency that each node achieved the same value as the C_{Global}. Node 101 has presented more than 300 times the same value that C_{Global} has for a clustering coefficient.

By these results, we observe the network dynamicity and the behavior of our proposed metric in relation to it. We identify that the metric can indicate individually the most vulnerable links in the network, but instead of using this information as absolute measure, the connectivity antifragility metric also ponders the existence of good connections between critical nodes and

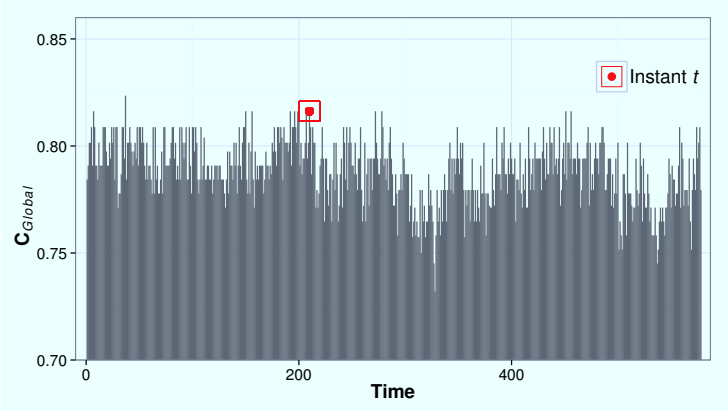

Figure 12: C_{Global} variation

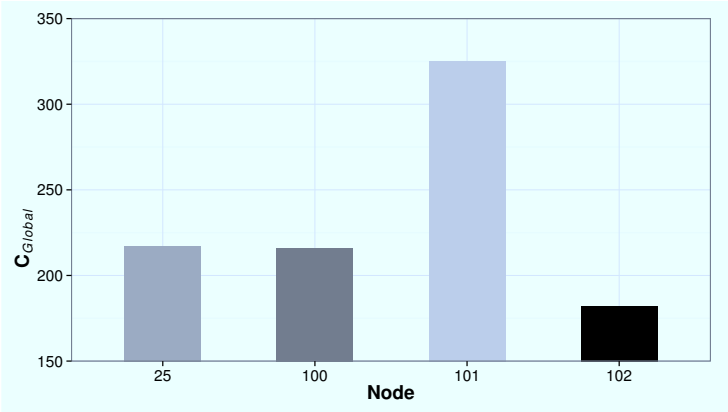

Figure 13: Frequency of nodes that determines C_{Global} value

their neighbors. This work pioneers by considering these two characteristics simultaneously and the results of this case study point out its potential.

6 Case study 2: Celular networks analyses

This section presents case study 2 applying the connectivity antifragility metric on a heterogeneous wireless network. In this case, we employ the metric over real traces from a heterogeneous cellular network. The trace files contained a list of latitude and longitude coordinates of each Base Transceiver Stations (BTSs). We developed a Python script for filtering and converting coordinates to fixed points in the network. The network is comprised of 191 BTSs scattered throughout Curitiba city's perimeter, South Brazil. Traces

are available at a public repository[4] by the Brazilian National Agency of Telecomunications (ANATEL). Five different service operators compose the network and they can employ different communication technologies, such as CDMA, WCDMA, 3G, and LTE to offer services for their users.

Fig. 14 shows the map of the city with the network formed by BTSs from different operators. Since different BTSs can employ heterogeneous technologies, each one results in diverse coverage areas. However, in this study, we investigate a scenario in which all BTSs have the same transmission radius of 2 KM, without lost in generalization for results and considering its coverage area modeled by a circle. The precise location of each BTS is indicated in the figure by the red mark, and colored circles represent its transmission coverage area. Each color represents a BTS from a specific service operator.

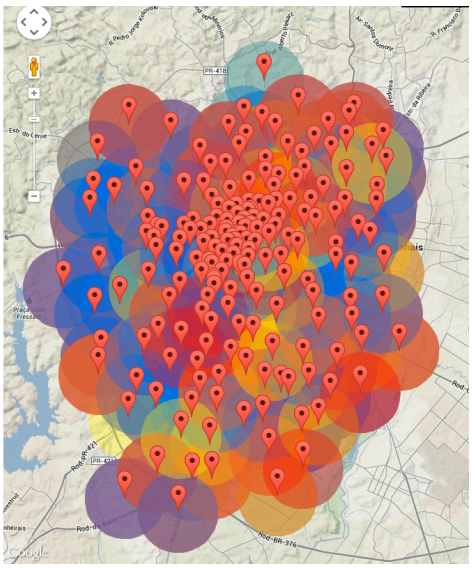

Figure 14: Celular BTSs location in Curitiba, South Brazil

From BTS locations and based on their coverage areas, we modeled the network by a graph in which BTSs are vertices and intersections between their coverage areas are edges. Differently from the case study 1, the graph representing the network is the same for different instants of time t, since BTSs are fixed. Fig. 15 shows the graph corresponding to the network. Furthermore, Fig. 16 shows the density of BTS by the physical area of the city. We observe that the network is very dense in downtown, represented in the figure by the dark region.

[4]http://sistemas.anatel.gov.br/stel/consultas/ListaEstacoesLocalidade/tela.asp?pNumServico=010

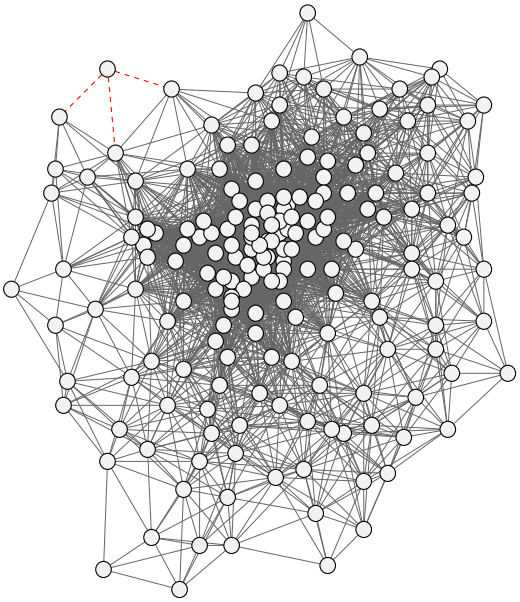

Figure 15: Cellular network graph

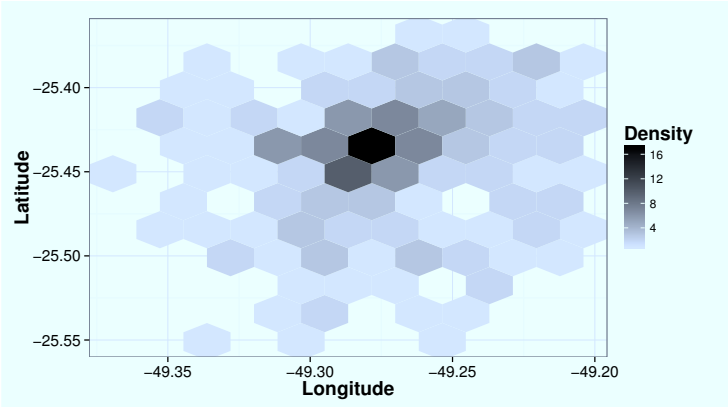

Figure 16: Density of vertices by the city perimeter

Fig. 17 presents the distribution of vertices' degree for the cellular network. Vertices' degrees vary from 3 to 80, and the average is about 58.19. We fit the vertices' degree behavior by a Poisson and Bernoulli probability density distribution with μ equal to 1.91. The observed behavior shows a small amount of vertices with a high degree and a huge amount of vertices with a very low degree. This degree distribution is the same found on different complex networks, including the degree distribution in the core of the Internet topology [Crespelle and Tarissan 2011].

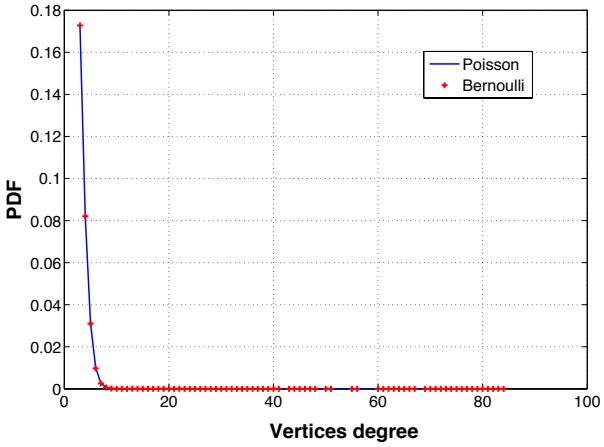

Figure 17: Vertices degree distribution

6.1 Results

For the graph presented in Fig. 15, we calculated T_c, the minimum cut tree, as shown in Fig. 18. In this graph, we want to highlight the great concentration of connections with a small amount of nodes, reinforcing observations performed by Fig. 16 and Fig. 17. Also, the zoomed part of the figure shows the minimum cut of T_c, presenting a size of 3. The edges in the minimum cut correspond to the dashed links in the graph of Fig. 15. We emphasize the fact that the minimum cut edges are in the periphery and not in the core of the network topology.

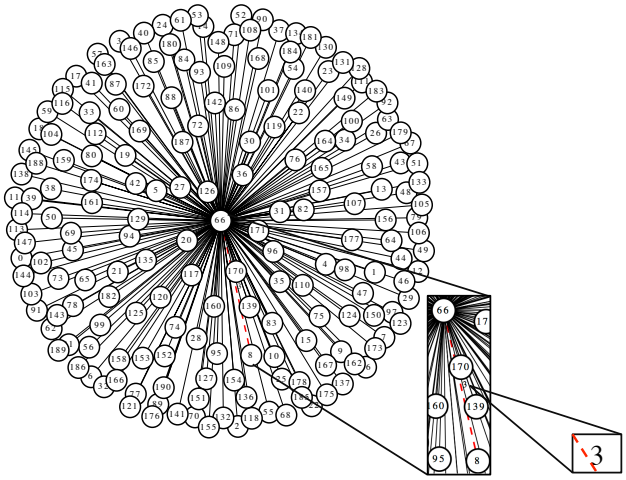

Figure 18: Minimun cut edges

Fig. 19 shows the CA calculated for the heterogeneous cellular network, varying the values of α and β. In this case study, the values of α are always higher than β, since we consider that the network fragility measure has a great impact in connectivity antifragility. Results show that CA increases as the value of α increases. On the scenario in which the value of α is 0.9 and β is equal to 0.1, the connectivity antifragility of the network is higher than 0.75, representing 75% of connectivity antifragility in the network. For the scenario in which the value of α is 0.6 and β equal to 0.4, the CA is up to 60%. Hence, we observe that the connectivity antifragility for the network varies from 60% up to 75%. We consider this behavior as result of the high connectivity among existing nodes composing the nodes highly connected in the network (the core of the network), what provides alternative paths to nodes communication.

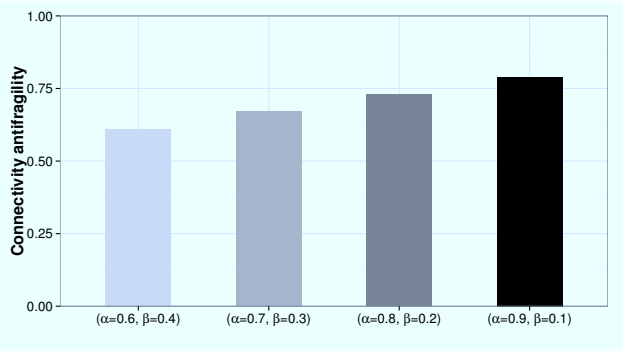

Figure 19: Connectivity antifragility of the heterogeneous cellular network

Table 2 shows the values of NF, FD, clustering and minimum cut calculated for the heterogeneous cellular network. We observe a small amount of minimal cutting size compared to the total amount of edges in the network. This situation results from the low density of edges in the network periphery, and different from the central region, that presented a high density, as illustrated in Fig. 16. As mentioned, the minimum cut of the network is located in the peripheral region, observed in Fig. 15. FD is calculated by the ratio between the minimum and maximun C_v belonging to the critical vertices in network. Its result indicates that, despite the unequal distribution of edges in the graph, the critical nodes present a high connectivity with their neighbors assisting in the network antifragility.

Table 2: Reults for cellular network

NF	**FD**	**Clustering**	**Minimum Cut**
0.15	0.75	0.5036	3

7 Conclusion

Complex networks and graph theory have been applied to different areas such as sociology, biology, physics, and computer science in order to understand the characteristics of non-uniformly random connectivity in real world networks. However, they have not been employed to analyze connectivity aspects in heterogeneous wireless networks considering the possibility of frequent disconnections of mobile terminals and availability issues. In this work, we proposed an innovative network measure called connectivity antifragility that describes the impact of each node or failure in network connectivity, providing the knowledge to learn from them and redesign network connections on real time. This measure allows the identification of the most vulnerable connections under failure or other disturbances. The metric was applied in two case studies, considering real traces from heterogeneous wireless networks. The first one considers a heterogeneous wireless mesh network, whose traces were available at the CRAWDAD web repository, whereas the second one addresses a real cellular network composed by base stations from five different providers. Results showed that the metric assists in identifying vulnerable connections in the network and provide knowledge that can be employed in solutions' proposals in order to keep the network resilient to disturbances. In future works, we envision applying this metric as a criterion for base station selection in mobility management and also based on it, to investigate the impact of network dynamism and mobility in network resilience.

Acknowledgment

This work was supported by CNPq and CAPES. Authors would like to thank Flavio Arieta, Guilherme Politta, Leonardo Melniski and Stephan Sumi.

References

[Ackley 2013] Ackley, D. H. (2013). Beyond efficiency. *Commun. ACM*, 56(10):38–40.

[Barrere et al. 2012] Barrere, M., Badonnel, R., and Festor, O. (2012). Towards the assessment of distributed vulnerabilities in autonomic networks and systems. In *IEEE NOMS*, pages 335–342.

[Cetinkaya et al. 2013] Cetinkaya, E., Peck, A., and Sterbenz, J. (2013). Flow robustness of multilevel networks. In *IEEE DRCN*, pages 274–281.

[Crespelle and Tarissan 2011] Crespelle, C. and Tarissan, F. (2011). Evaluation of a new method for measuring the internet degree distribution: Simulation results. *Comput. Commun.*, 34(5):635–648.

[Gardner et al. 2013] Gardner, M., Beard, C., and Medhi, D. (2013). Using network measure to reduce state space enumeration in resilient networks. In *IEEE DRCN*, pages 250–257.

[Ghosh et al. 2012] Ghosh, A., Mangalvedhe, N., Ratasuk, R., Mondal, B., Cudak, M., Visotsky, E., Thomas, T. A., Andrews, J. G., Xia, P., Jo, H. S., Dhillon, H. S., and Novlan, T. D. (2012). Heterogeneous cellular networks: From theory to practice. *IEEE Commun. Mag.*, 50(6):54 –64.

[Hashim et al. 2012] Hashim, F., Munasinghe, K., and Jamalipour, A. (2012). On the negative selection and the danger theory inspired security for heterogeneous networks. *IEEE Wireless Commun.*, 19(3):74–84.

[Heegaard and Trivedi 2009] Heegaard, P. E. and Trivedi, K. S. (2009). Network survivability modeling. *Computer Networks*, 53(8):1215–1234.

[J. and M'Raïhi 1999] J., M. and M'Raïhi, D. (1999). Mix-based electronic payments. In *Proc. of the Selected Areas in Cryptography*, pages 157–173, London, UK, UK. Springer-Verlag.

[Manzano et al. 2013] Manzano, M., Calle, E., Ripoll, J., Fagertun, A., and Torres-Padrosa, V. (2013). Epidemie survivability: Characterizing networks under epidemic-like failure propagation scenarios. In *IEEE DRCN*, pages 95–102.

[Qin et al. 2013] Qin, Z., Denker, G., Talcott, C., and Venkatasubramanian, N. (2013). Achieving resilience of heterogeneous networks through predictive, formal analysis. In *ACM HiCoNS*, pages 85–92.

[Sterbenza et al. 2010] Sterbenza, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Scholler, M., and Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 58(1):1245–1265.

[Tseitlin 2013] Tseitlin, A. (2013). The antifragile organization. *Commun. of the ACM*, 56(8):40–44.

[Venmani et al. 2013] Venmani, D. P., Gourhant, Y., and Zeghlache, D. (2013). Openroutes: augmenting backhaul network survivability with reduced redundancy - a topology. In *MobiCom*, pages 183–186.

[Zhang et al. 2008] Zhang, C., Song, Y., and Fang, Y. (2008). Modeling secure connectivity of self-organized wireless ad hoc networks. In *IEEE INFOCOM*.

[Zhang and Sundaram 2012] Zhang, H. and Sundaram, S. (2012). Robustness of complex networks with implications for consensus and contagion. In *IEEE CDC*, pages 3426–3432.