



Vulnerability of public transportation networks against directed attacks and cascading failures

Antonio Candelieri^{1,2} · Bruno G. Galuzzi¹ · Ilaria Giordani^{1,2} · Francesco Archetti^{1,2}

Accepted: 24 December 2018 / Published online: 19 February 2019
© The Author(s) 2019

Abstract

This paper presents some results devoted to providing network analysis functionalities for vulnerability assessment in public transportation networks with respect to disruptive events and/or targeted attacks to stations. The results have been obtained on two public transportation networks: the bus network in Florence, Italy, and the transportation network in the Attika region, Greece. The analysis implements a topological approach, based on graph theory, using a multi-graph to model public transportation networks and analyse vulnerabilities with respect to the removal of one or more of their components. Both directed attacks and cascading failures are considered. While the first type of disruptive events is related to a static analysis, where nodes are removed according to a rank related to some centrality measures, the second type is related to a dynamic analysis, where a failure cascade is simulated making unavailable the node with the highest betweenness value. Vulnerability measures are computed as loss of connectivity and efficiency, with respect to both the two different types of disruptive events considered. This study allows to evidence potential vulnerabilities of the urban networks, that must be considered to support the planning process into the creation of resilient structures.

Keywords Public transport system · Network analysis · Vulnerability · Cascading failure

✉ Bruno G. Galuzzi
bruno.galuzzi@unimib.it

Antonio Candelieri
antonio.candelieri@unimib.it

Ilaria Giordani
ilaria.giordani@disco.unimib.it

Francesco Archetti
francesco.archetti@unimib.it

¹ Department of Computer Science, Systems and Communications, University of Milano-Bicocca, viale Sarca 336, 20125 Milan, Italy

² Consorzio Milano-Ricerche, via Roberto Cozzi, 53, 20126 Milan, Italy

1 Introduction

In these last years, the planning processes for urban transport have focused the attention on the creation of urban networks characterized by high connectivity and interrelation between their components. However, this can cause potential vulnerabilities because the functionality of each component now depends on an ever-increasing number of other infrastructure components. The fail of an infrastructure component can cause significant damages, in terms of temporary disconnection of parts of the networks and/or decrease of the level of its efficiency. The protracting of failure can carry the original failure over to successive components.

This paper stems from the activities of the European H2020 project *RESOLUTE* (RESilience management guidelines and Operationalization applied to Urban Transport Environment), whose general aim is the operationalization of the resilience/vulnerability concepts into a set of guidelines and related software for assessing vulnerability and resilience in a wide variety of conditions (Bellini et al. 2017).

The term resilience, from its Latin root “resilire”, means—loosely speaking—the capability of a system, both natural or man-made, to resist, rebound or spring back in response to endogenous events (e.g. component failures) or exogenous (natural or man-made) attacks. Resilience means different things to different scientific and professional communities and is being addressed under different names; indeed, it came to define a set of properties of a much broader socio-technical framework to cope with infrastructure threats and disruptions including preparedness, response, recovery and adaptation. Thus, different tools are needed to analyse and support decisions for anticipation, prevention, mitigation and restoration, depending on different types of disruptions (Ferreira and Simoes 2015; Gaitanidou et al. 2015; Gaitanidou and Tsami 2016; Archetti et al. 2015).

This paper is focused on *public transportation networks* (PTNs) using tools from network science and OR to analyse vulnerability and a restricted meaning of resilience, namely the levels of flexibility and capacity to ensure the persistence of key functions even in the presence of cascading failures. Vulnerability in its different forms is the key concept we use to analyse the network structure (Mattsson and Jenelius 2015). In the last years, studies on the vulnerability of the PTNs attract a growing attention because of the possible repercussions that incidents can have on the day-to-day functioning of a city. Recent studies about vulnerability of PTN can be found in Rodríguez-Núñez and García-Palomares (2014), Cats and Jenelius (2015, 2018), Zhang et al. (2015) and Cats et al. (2016).

Methods of representation and analysis of vulnerability come from several different communities like water distribution systems (Soldi et al. 2015; Candelieri et al. 2015), transportation systems (Berdica 2002), optimization (Ash and Newth 2007), internet (Cohen et al. 2000) and engineering design (Agarwal et al. 2003).

Coherently with the aim of RESOLUTE to provide a toolbox of wide utilization, a topological approach has been adopted in this paper, based on the description of a PTN using *graph theory*. To model multiple lines/routes between two

stations/stops, a multi-graph representation of a PTN is used (Von Ferber et al. 2009b), and specific attributes/labels are adopted to distinguish two or more edges connecting two nodes. This approach offers the benefit of not requiring a huge amount of data—typically the only information about the interconnections is needed to create the graph associated to the PTN infrastructure and still they can provide fundamental insights about the vulnerability of a transport network.

The term vulnerability is related to the capability of a PTN to resist to a disrupting event, consisting of the removal of one or more of its components. In the extensive literature about attack strategies, an attack is done removing nodes (Von Ferber et al. 2009a; Berche et al. 2010) or edges (Jenelius and Cats 2015; Jenelius and Mattsson 2015), using both randomly and targeted selection, and considering a static (Von Ferber et al. 2009a) or dynamic (Zou et al. 2013) analysis. In this paper, we focus on targeted attacks based on the removal of a node or a group of nodes. In the static approach we specifically remove subsequently nodes according to a list defined a priori. In the dynamic approach we remove a specific node and, under the condition of a network capacity limit, we analyse the consequently cascading failure (Zou et al. 2013) caused by the possible redistribution of the load on the whole network. In this last case, the removal of a node is done but the routes passing through it are maintained, as described in Sect. 5.2. To measure the variations of the graphs, the network efficiency (Latora and Marchiori 2001) and the relative size of the largest component (Von Ferber et al. 2009a) are considered.

In this paper, we analyse the urban PTNs of Florence (Italy) and the Attika region (Greece), the use cases of the RESOLUTE project. An a priori-vulnerability analysis of the two PTNs is done using different elements from network analysis and spectral analysis. Then two different attack simulations are considered. The first is a targeted attack in which the nodes are removed according to two different lists measuring different values of the centrality measures in descending order; the second is a cascading failure starting from the node with the highest betweenness value.

The main contribution of this study is to analyse two real-complex PTNs studying their vulnerability and the resilience to different attack strategies by means of graph theory and network analysis. The used graph representation can be generalized to any PTN, if the interconnection data are provided by, e.g. the GTFS repository (Google 2018). The computational results can be obtained using any programming code able to threat efficiently information coming from graph representation. In this study, the GraphStream (University de le Havre 2010) library was particularly used to model a PTN, while the attack strategies and the network's analysis were implemented in Java.

Another important contribution is about the way to simulate the cascading failure in the dynamic approach. The choice to maintain the routes passing through an unavailable station has been made to simulate a real-transport situation in which it is possible to simply “jump” that station moving from one station to another one of a line/route. This fact implies the re-computation of the nodes loads of the networks, in a different way from the traditional approaches to the cascading failure.

The structure of this paper is as follows. Sect. 2 presents the main elements of the graph model and in particular basic tools like spectral analysis and the centrality measures. Section 3 introduces the concept of vulnerability and its different

mathematical models. Section 4 introduces attack strategies to networks, considering in particular targeted attacks and cascading failures. Section 5 shows how the previous modelling tools can be used to model a PTN focusing on two-real life PTNs. A contextualization of the attack strategies for real PTN is provided. Finally, Sect. 6 is about the computational analysis of efficiency and resilience, among other, in static conditions and subsequently in the failure cascading framework.

2 Background info

2.1 Basic concepts and notation

From a mathematical point of view, a graph is a mathematical object $G = (V, E)$, where $V = \{1, 2, \dots, n\}$ is the set of *nodes* and E is the set of *edges*. Each edge of G is represented by a pair of nodes (i, j) with $i \neq j$, and $i, j \in V$ and $i, j = 1, \dots, n$. If $(i, j) \in E$, i and j are called *adjacent*, or *neighbours*. Any of the edges having i as one of its nodes is called *incident* on i . In case of multiple edges between a pair of nodes (*multi-graph*), it is not possible to identify an edge only by its nodes, but it is necessary to use specific attributes, e.g. names, that characterize and distinguish each edge by another edge, represented by the same pair of nodes.

The number of neighbours of a node i , denoted by d_i , is called *node degree*. We denote with $\delta(G)$ and $\Delta(G)$ the minimum and the maximum degree of the nodes of G , respectively.

The adjacency relationship between the nodes of G is represented through a non-negative $n \times n$ matrix A , called *Adjacency Matrix* of G . The entry $A_{ij} = 1$ if i and j are adjacent nodes, and 0 otherwise. The adjacency matrix can be used also for multi-graphs and graphs with loops, by storing the number of edges between two vertices in the corresponding matrix element, and by allowing nonzero diagonal elements.

If all the nodes of G are pairwise adjacent, then G is called *complete*. A graph G is *undirected* if (i, j) and (j, i) represent the same edge, and it is *simple* if it is undirected, without self-loops (edges starting from a node and ending on the same node) and only one edge can exist between each pair of nodes (i, j) , with $i \neq j$. Undirected graphs have the properties that $A_{ij} = A_{ji}$ if $i \neq j \forall i, j \in V$. Simple graphs have the properties that $A_{ii} = 0, \forall i \in V$.

A measure that quantifies how much the nodes of the graph are connected among them, is the *density* (q). Given a graph $G = (V, E)$, its density is simply computed as the ratio between the number of edges of the graph, $m = |E|$, and the overall possible number of connections among the $n = |V|$ nodes of G (i.e. $n(n - 1)/2$ in case of undirected graphs):

$$q = \frac{2m}{n(n - 1)}, \quad (1)$$

The metric structure of a complex graph is related to the topological distance between its nodes, written in terms of walks and paths in the graph. A *walk* (of length

k) in G is a non-empty alternating sequence $\{i_1, l_1, \dots, i_{k-1}, l_{k-1}, i_k\}$ of nodes and edges such that $l_r = (i_r, i_r + 1)$ for all $r < k$. If $i_1 = i_k$ the walk is *closed*. A *path* from i to j is a sequence of distinct adjacent nodes starting from i and ending to j , in which each node is visited only twice.

A *connected graph* is a graph where a path exists between each pair of nodes $i, j \in V$, otherwise it is called disconnected. The length of a path is the number of edges of that path. If $i, j \in V$, a *geodesic* between i and j is a path of the shortest length that connects i and j . The length of a geodesic between i and j is called *distance* $d_{i,j}$. The maximum distance $D(G)$ between any two vertices in G is called the *diameter* of G .

A *subgraph* $G' = (V', E')$ of G is a graph such that $V' \subseteq V$ and $E' \subseteq E$; a *connected component* of G is a maximal connected subgraph of G .

2.2 Spectral analysis

The use of spectral methods in graph theory has a long tradition (Bonacich 1972). Specifically, spectral graph theory studies the eigenvalues of matrices that embody the graph structure. One of the main objectives in spectral graph theory is to deduce structural characteristics of a graph from such eigenvalue spectra.

In case of undirected graphs, the adjacency matrix $A(G)$ is symmetric and all its eigenvalues are real. The eigenvalues $\mu_1(G) \leq \mu_2(G) \leq \dots \mu_n(G)$ of $A(G)$ are called the *spectrum* of G . The eigenvalue spectra of a graph provide valuable information about its structure and static properties. The largest eigenvalue of the adjacency matrix $\mu_n(G)$ is called *spectral radius* of G and is denoted by $\rho(G)$. An important property is given by the following inequality

$$\sqrt{\Delta(G)} \leq \rho(G) \leq \Delta(G), \tag{2}$$

that relates the spectral radius with the maximum degree of the nodes.

The difference $s(G) = \rho(G) - \mu_{n-1}(G)$ between the spectral radius of G and the second eigenvalue of the adjacency matrix $A(G)$ is called the *spectral gap* of G (Estrada 2006). A small value of $s(G)$ is usually observed through low connectivity, and the presence of bottlenecks and bridges whose removal cut the graph into disconnected parts.

The *Laplacian matrix* of G is an $n \times n$ matrix $L(G) = D(G) - A(G)$, where $D(G) = \text{diag}(k_i)$ and k_i denotes the degree of the node i . The matrix $L(G)$ is positive semi-definite in case of a simple graph. The eigenvalues of $L(G)$ are called the Laplacian eigenvalues of G . The Laplacian eigenvalues $\lambda_1(G) = 0 \leq \lambda_2(G), \dots \leq \lambda_n(G)$ are all real and nonnegative. The smallest eigenvalue is always equal to 0 with multiplicity equaling the number of connected components of G . The second smaller eigenvalue is called the *algebraic connectivity* of G . Algebraic connectivity is one of the most broadly extended measures of connectivity. Larger values of algebraic connectivity represent higher robustness against efforts to disconnect the graph, so the larger it is, the more difficult it is to cut a graph into independent components. An important inequality for the algebraic connectivity is given by

$$\lambda_2(G) \leq \frac{n}{n-1} \delta(G), \tag{3}$$

that relates it with the minimum degree of the nodes. In case of connected graphs, also the following inequality can be found

$$\lambda_2(G) \geq \frac{4}{n \cdot D(G)}, \quad (4)$$

that relates the algebraic connectivity with the diameter of the graph and its size.

2.3 Network-based centrality measures

In computer science and network science, network theory is a part of graph theory. A network can be defined as a graph in which nodes and/or edges have attributes (e.g. names). Networks from different domains share some properties that can be measured by a set of indices, called *centrality measures* (Albert and Barabási 2002), which can take specific ranges of values in correspondence of each specific domain. Centrality concepts were first developed in social network analysis, and many of the terms used to measure centrality reflect their sociological origin. These indices answer the question “*What characterizes an important vertex?*”. The answer is given in terms of a real-valued function on the nodes of a graph, where the values produced are expected to provide a ranking which identifies the most important nodes.

Historically the first and conceptually simplest measure is *degree centrality* based on the idea that important nodes are those with the largest number of links to other nodes in the graph. The degree centrality of a node i is defined as

$$D_c(i) = d_i. \quad (5)$$

The degree can be interpreted in terms of the immediate risk of a node for catching whatever is flowing through the network (such as a virus, or some information).

Another important centrality measure is the *betweenness centrality* (Freeman 1977) that quantifies the number of times a node acts as a bridge along the shortest path between two other nodes. The betweenness can be represented as

$$B_c(i) = \frac{1}{n(n-1)} \sum_{j \neq i \neq k} \frac{\sigma_{jk}(i)}{\sigma_{jk}}, \quad (6)$$

where σ_{jk} is the total number of shortest paths from the node j to node k and $\sigma_{jk}(i)$ is the number of those paths that pass through i .

3 Vulnerability analysis of a network

The concept of vulnerability in a complex network aims at quantifying its security and stability under the effects of any type of dysfunctions. Different approaches from different branches of knowledge can be introduced to quantify the vulnerability of a complex network.

In complex transportation systems, the vulnerability can be related to the susceptibility to disruptions giving a considerable reduction in network serviceability as a

result (Mattsson and Jenelius 2015). An often cited and representative definition of vulnerability in a road transportation system can be found in (Berdica 2002): “*Vulnerability in the road transportation system is a susceptibility to incidents that can result in considerable reductions in road network serviceability*”. This definition can be generalized to other modes of transport and emphasises that there is an initiating *disruptive event*, that the fundamental purpose of the transport system is hurt, and that the adverse consequences are significant.

An important way to deal with the vulnerability analysis of transport networks is the *topological approach*. In this approach a real transport network is represented in the form of an abstract graph, in which the nodes and links have specific counterparts in the real network. The used graph can be directed or undirected and unweighted or weighted according to the application in mind.

The performance of the network after the removal of nodes/links is often evaluated as the change of the important quantities. The first is the *Latora and Marchiori network efficiency* (E) (Latora and Marchiori 2001) and is defined as

$$E = \frac{1}{n(n-1)} \sum_{i,j \in V, i \neq j} \frac{1}{d_{ij}}, \tag{7}$$

where d_{ij} represents the distance between nodes i and j . Normalization by $n(n-1)$ ensures that $E \leq 1$, in case of an unweighted graph. The maximum value, $E = 1$, is assumed only when the graph is complete. However, graphs representing real-world networks can, nevertheless, assume high values of E . A significant vulnerability of a network will correspond to a significant decrease of E , in case of the removal of a node or some nodes.

The second and complementary performance indicator is the *relative size of the largest component* (S) (Von Ferber et al. 2009a; Berche et al. 2010; Mattsson and Jenelius 2015), that considers the relative size of the largest connected component

$$S = \frac{N_1}{N}, \tag{8}$$

where N and N_1 are the numbers of nodes of the network and of its largest component, respectively. As we will see, a vulnerable network will correspond to a significant decrease of S , in case of the removal of a node or some nodes.

3.1 Vulnerability analysis using the degree distribution

A useful property to analyse the vulnerability of a network is to consider its degree distribution: if it follows a power-law, at least asymptotically, it means the fraction $P(d)$ of nodes in the network with a degree d goes from large to low values of d as

$$P(d) \approx d^{-\gamma}, \tag{9}$$

where γ is a parameter whose value is typically in the range $2 < \gamma < 3$. If the degree distribution follows a power law then the network is called *scale-free* (Onnela et al.

2006), and many man-made and natural complex networks have been reported to be scale-free (Virkar and Clauset 2014). The most notable characteristic in a scale-free network is the relative commonness of nodes, named *hubs*, with a degree that greatly exceeds the average. These hubs are thought to be important in the analysis of vulnerability of the network. Indeed, the removal of a few major hubs could cause the disconnection of the network and the creation of a set of rather isolated graphs.

3.2 Vulnerability analysis based on fall of efficiency

A way to measure the vulnerability of the network is using the loss of efficiency (Latora and Marchiori 2007; Criado and Romance 2012) observed when we remove some nodes that potentially increase the value of the distances between the nodes of the network. These types of measures are based on the idea that the importance of a node, or a group of nodes, is related to the ability of the network to respond to the removal of that node, or group of nodes, from the network. If G is the graph representing the network, the relative drop in the network efficiency caused by the removal of a node i from the graph is defined as

$$C_{\Delta}^E(i) = \frac{E(G) - E(G \setminus \{i\})}{E(G)}, \quad (10)$$

where $G \setminus \{v\}$ denotes the network G without the node i . The loss of efficiency of the graph G is defined as

$$V_E(G) = \max_{i \in V} C_{\Delta}^E(i), \quad (11)$$

that measures the worst performance of Eq. (10) in case of a possible attack on a node of the network. In this case, the greater the value V_E , the greater is its vulnerability.

3.3 Vulnerability analysis based on centrality measures

A second way to measure the vulnerability of the network is based on the measures related to betweenness centrality and, as in (Criado and Romance 2012) and (Boccaletti et al. 2007), is defined as

$$V_{B,p}(G) = \left(\frac{1}{n} \sum_{i \in V} B(i)^p \right)^{1/p}, \quad (12)$$

where $p \in [1, +\infty]$. These p -functions are based on the idea that the distribution of the number of minimal paths between the nodes influences the vulnerability of the network. In this case, the greater the value $V_{B,p}$, the lower is its robustness.

3.4 Vulnerability analysis using spectral analysis

There is no specific formula, contrary to those reported in the previous subsections, linking spectral analysis to a measure of vulnerability related to the removal of a node. However, both algebraic connectivity λ_2 and spectral gap s are indicators of difficulty to split the graph (Criado and Romance 2012). The larger the algebraic connectivity, the more difficult it is to disconnect the graph. A large value of the spectral gap, together with a uniform degree distribution results in higher structural sturdiness and robustness against node and link failures. On the contrary, low values of the spectral gap indicate a lack of good expansion properties usually represented by bridges, and network bottlenecks. Since the measure of spectral analysis can be related to the connectivity, they can be related to S .

4 Directed attacks and cascading failure

In general, from the perspective of structural vulnerability, it is possible to study how the characteristics of a complex network change when some of its elements are removed. Below, we will call such removal an attack (Berche et al. 2010).

In practice, the origin of the attack and its scenario may differ to large extent, ranging from a *random attack*, when a node or a group of nodes is removed at random to a *targeted attack*, when one or more of the most influential network nodes are removed according to their operating characteristics.

Once a node, randomly or targeted, is attacked and removed from the network, there are two different ways to continue and/or analyse the attack: the *static approach* (Von Ferber et al. 2009a), and the *dynamic approach* (Zou et al. 2013).

In the static approach, the failure of a node is assumed not to cause other nodes to fail. In this case, to analyse the possible collapse of the whole network, it is possible to remove all the nodes one by one, choosing randomly or according to a certain criterion, preparing a list of the nodes for the initial network and removing the nodes according to this list (Holme et al. 2002; Berche et al. 2010; Latora and Marchiori 2005). To quantify such importance of a node i and, so, its position in the list, it is possible to consider measures related to the degree or the betweenness centrality, previously analysed in Sect. 2.3. The use of such measures can be justified by the fact that we have seen their importance in the definition of the vulnerability of a network.

During an attack, one can single out different impacts related to the effectiveness of a network and its vulnerability during an attack. This can be done measuring, for example, the values of E and S till all nodes in the network are removed, obtaining two curves, $S(c)$ and $E(c)$, where c represents the fraction of the removed nodes.

In the dynamic approach of a network attack, it is assumed that the removal of the node can cause other nodes to fail. Under the condition of a network capacity

limit, a node failure will lead to load redistribution of the whole network, thus making a load of some nodes exceed its capacity and causing the possible failure of other nodes. In particular, infrastructure networks with complex interdependencies are known to be vulnerable to *cascading failures* (Ash and Newth 2007; Gutfraind 2012; Zou et al. 2013).

A cascading failure is a domino effect which originates when the failure of a given node triggers subsequent failures of one or several other nodes, which in turn trigger their own failures. Thus, the number of failed or stressed nodes increases, propagating throughout the network. Examples of cascading failures in the real world are, for example, a wide-scale power outage or the previous global economic crisis.

A simple model for a cascading failure on a network assumes that each node transmits one unit of some quantity (energy, information, the volume of passenger, etc.) to every other node through the shortest path between them. As a result, each node i is characterized by a certain *load* L_i , that describes some quantity able to describe the importance of the node in the network. Example of these quantities can be the centrality measures. In particular, a common choice is to use the value of the betweenness centrality B_i , which represents the number of shortest paths passing through that node, as we see in Sect. 2.3.

Each node i is characterized by a given *capacity* ψ_i , which is the maximum load that can be handled by that node. A natural assumption is that the capacity assigned to a node is proportional to the load that it is expected to handle, since cost constraints prohibit indiscriminately increasing a node's capacity

$$\psi_i = (1 + \alpha) \cdot L_i(0) \forall i \in V^0 \quad (13)$$

where $\alpha \geq 0$ is a tolerance parameter which quantifies the excess load that a given node can handle, and V^0 is the set of nodes of the original graph.

Cascading failures are initiated when a heavily loaded node is lost for some reason, and the load on that node must be redistributed to other nodes in the network. The removal of the node simulates the loss of the node. The redistribution of the load to the other nodes in the network requires the re-computation of the load value $L_i(t+1)$ for each node i . This re-computation can radically alter the values of the loads on the network. Certain nodes can have a load smaller than their previous value, and some others can have a higher one. In particular, if a node i has a new load $L_i(t+1) > \psi_i$, then this node also fails. These failures can, in turn, trigger more failures, thus leading to a cascade. The process iterates until no more nodes must be removed from the network, that means when an iteration \bar{t} exists, for which

$$L_i(\bar{t} + 1) \leq \psi_i \quad \forall i \in V^{\bar{t}} \quad (14)$$

where V^t is the set of nodes of the network, at iteration \bar{t} , with $V^{\bar{t}} \subseteq \dots \subseteq V^0$.

To describe the severity of a cascade, during and at the end of the process, it is possible to consider the value of E and S , computed for each step t of the cascade, obtaining two curves, $S(t)$ and $E(t)$.

5 PTNs as graphs and networks

5.1 Modelling a PTN as a complex network

The main elements of a PTN can be mapped into graph elements, basically nodes and edges. Although everyone has an intuitive idea of what a PTN is, it appears that there are numerous ways to define its topology (Berche et al. 2010). A straightforward representation of a PTN as a graph, models every station by a node while edges correspond to the links that exist between stations according to the PT routes servicing them (Fig. 1, a). By this way, the full information about the network of N stations and R routes is given by the set of ordered lists each corresponding to one route or one of the two directions of a given route. Multiple entries of a given station in such a list are possible and do occur. A simple graph that represents the situation is in Fig. 1 a). This graph represents each station by a node, a link between nodes indicates that there is at least one route that services the two corresponding stations consecutively. No multiple links are allowed. The space of such type of graphs is called L -space. Extending the notion of L -space one may either introduce multiple edges between nodes depending on the number of services between them. Such graph-space is called L' -space (Fig. 1, b)) (Von Ferber et al. 2009b), and it is the space we use in this paper.

The network-based centrality measures represent important characteristics of a PTN. The degree centrality measures the importance of a station in terms of possible interconnection between other stations and/or lines. The betweenness centrality is interpreted as a measure of the volume of passengers that transit through it if we imagine that a passenger chooses the shortest path to go from one point to another one of the PTN. Note that a high volume of passengers (high value of betweenness centrality) does not always imply a high level of interconnection (high value of degree centrality). A possible case can be a bridge station connecting the central part of a city with one of its peripheral parts.

5.2 Disrupting events in a PTN

Disruptions of a PTN can be of different types (accidents, infrastructure collapses and attacks...) and can lead to impacts of different severity: injuries, fatalities. Common

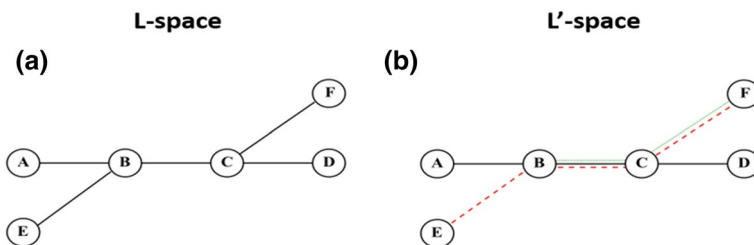


Fig. 1 A piece of public transport map, in which Stations A-F are serviced by two lines (the black solid and red dashed line, respectively). Such map is represented using **a** the L -space, and **b** the L' -space

disruptions, such as a blocked road link, a rail service interruption, a strike, and so forth, have an impact on lower severity.

In the following, a relevant real-world event towards graph modifications is considered: the *closure of a station/stop*. The simulation of such closure is classically done by removing the corresponding node and all the links having this node as vertex. Let $G = \langle V, E \rangle$ denote the original graph associated to the PTN and $k \in V$ the target node (i.e. the station/stop to close). The resulting graph after this event is $G' = \langle V', E' \rangle$ where: $V' = V \setminus \{k\}$ and

$$E' = E \setminus \dot{E} \tag{15}$$

where:

$$\dot{E} = \{(i, j) \in E : i = k \vee j = k\}.$$

Another possible way to simulate the closure of a station can be done removing a node but maintaining the transport lines/route passing through it. Therefore, new possible links are built to maintain all the lines after the removal of the nodes (Fig. 2b). The resulting graph after this event is $G' = \langle V', E' \rangle$ where: $V' = V \setminus \{k\}$ and

$$E' = (E \setminus \dot{E}) \cup \ddot{E} \tag{16}$$

where:

$$\dot{E} = \{(i, j) \in E : i = k \vee j = k\}$$

$$\ddot{E} = \{(i, j) | i, j \in V \wedge (i, k) \in E \wedge (k, j) \in E\}$$

While the first case is the classical way to analyze the effect of a targeted attack in a static context (Von Ferber et al. 2009a), the latter is considered in a dynamic context, as we will see in the next section. In this last case, if a station is unavailable the urban transport simply “jumps” that station.

In the context of urban transport, the cascading failure can represent an example of domino effect related to the disablement/closure of a station characterized, e.g. by a high volume of passengers (high value of betweenness), that transit through it. The closure of a station modifies the passengers’ routes (shortest parths)

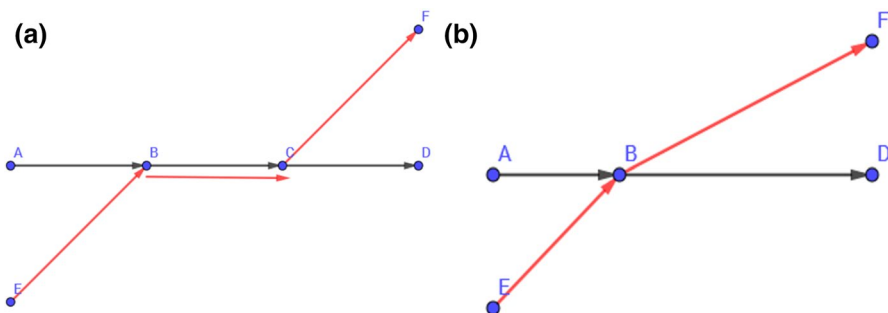


Fig. 2 A piece of public transport line, before (a) and after (b) the closure of the station C, but maintaining the routes, as described in Eq. (16)

deeply and, in case of preservation of the routes (Eq. 16), the volume of passengers of the disabled station is re-distributed between the other stations of the line/route. In this case, if one station exceeds the maximum quantity of passengers (load), also this station could be disabled, creating a cascading failure.

5.3 Case studies

In this section, we describe the two PTNs analyzed in this paper. Besides, the two PTNs are modelled through a directed multi-graph, because more than one route/line may connect two stations. The first PTN considered is the public bus transportation in Florence. This city is one of the biggest towns in central Italy, with a population of about 400,000 inhabitants and a surface of about 100 km². The public transportation system is done by a single operator, named ATAF, and consists of about 50 bus lines, for a total number of 999 bus stops. Figure 3, a) and b) shows the corresponding graph, consisting of 999 nodes and 3226 edges. To improve the visualization, we did not draw multiple edges between two nodes.

The second PTN considered is bigger than the first one and consists of the public transportation network of the Attika region. This region is located on the eastern edge of Central Greece and covers about 3.808 km². In addition to Athens, it contains within its area the cities of Piraeus, Eleusis, Megara, Laurium, and Marathon, as well as a small part of the Peloponnese peninsula and some islands. About 3,750,000 people live in the region, of whom more than 95% are inhabitants of the Athens metropolitan area.

The PTN of the Attika region includes bus, tramway and subway, for a total number of about 277 lines and 7681 stops. Figure 3a, b shows the corresponding graph, consisting of 7681 nodes and 18,128 edges. Again, to improve the visualization, we did not draw multiple edges between two nodes.

The two networks analyzed are either operated by a single operator (Florence) or by a small number of operators (Attika) with an appropriate coordination. Rather than artificially dividing these centrally organized networks into

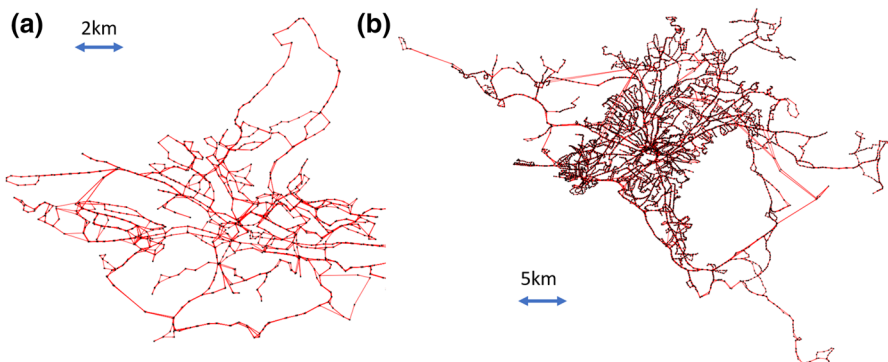


Fig. 3 **a** The graph associated to the PTN of Florence. The black points correspond to the nodes (stops) of the network, whereas the red lines represent the edges (links). **b** The graph associated to the PTN of the Attika region

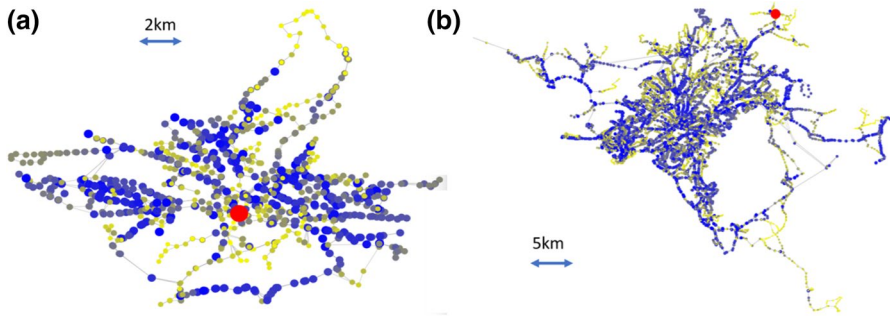


Fig. 4 The value of betweenness for the nodes associated to the PTN of Florence (a) and Attika (b). From yellow to blue and for small to large size of the nodes the value of the betweenness increases. The bigger red points indicate the nodes with the highest betweenness

subnetworks of different means of transport like bus and metro or in an ‘urban’ and a ‘sub-urban’ part, we treat each full PTN as an entity.

Figure 4a, b shows the two graphs in which the value of node betweenness is highlighted. The biggest red points indicate the nodes with the highest betweenness.

In Attika’s PTN, the peculiar location of the node with highest betweenness depends on the fact that the PTN has more branches towards peripheral regions, with many sub-graphs (i.e. clusters) associated with the peripheral areas, connected to the center of the network by nodes characterized by high values of betweenness (all the paths between two clusters pass through them). Thus, several nodes with high betweenness values are located on the branches connecting peripherals.

6 Analysis of two real-world PTNs

6.1 A priori vulnerability analysis

To start the analysis of the two PTNs, we compute some quantities associated to their original graph, without considering any possible damage, or faultless. For simplicity, for these analyses, we have threaded the two PTNs as undirected graphs.

Table 1 reports some values previously described in Sect. 2.1. Both the PTNs have a minimum degree equal to 1, and a similar value of the maximum degree.

Table 1 The value of the minimum, the maximum, the average and the standard deviation of the degree distribution of the two networks, and the value of density and the diameter

| City | $\min(d_k)$ | $\max(d_k)$ | \bar{d}_k | $\sigma^2(d_k)$ | q | D |
|---------------|-------------|-------------|-------------|-----------------|-------|-----|
| Florence | 1 | 40 | 6.46 | 5.23 | 0.006 | 53 |
| Attika region | 1 | 38 | 4.72 | 3.86 | 0.001 | 142 |

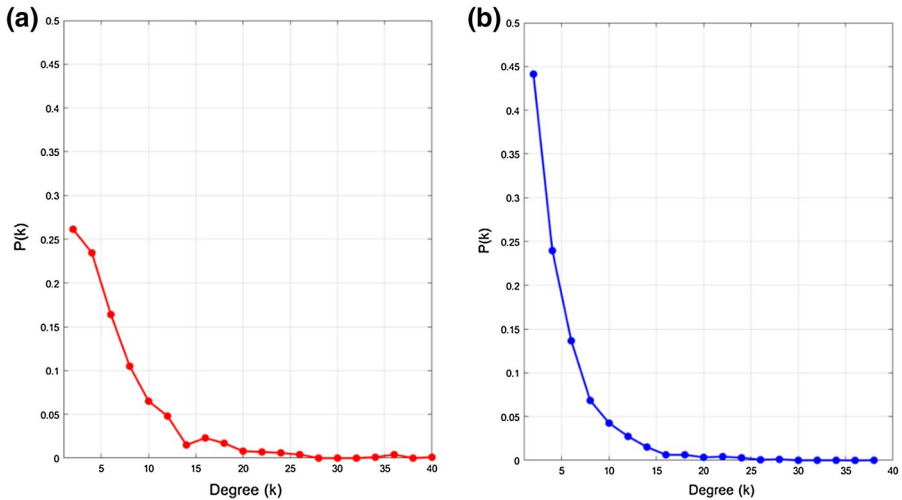


Fig. 5 **a** Degree distribution of the PTN of Florence. **b** Degree distribution of the PTN of the Attika region

However, the average degree and standard deviation of Florence's PTN is greater than the Attika's one, according to the greater value of density.

Figure 5 shows the degree distribution of the two PTNs. Both the PTNs have a degree distribution like a power-law distribution, more evident in the case of Attika.

Regarding the connectivity, at first glance both PTNs have a low value of the algebraic connectivity: 0.008 for Florence and 0.001 for Attika. Thus, even if the associated graphs are connected, they are not very robust to node or edge failures. Indeed, to disconnect the graph, it is sufficient to remove just one node.

An important difference between the two networks is the value of the spectral gap s : 2.21 for Florence and 0.32 for Attika, respectively; the lower value of s for Attika is in accordance with the presence of many bottlenecks and bridges (for example, the nodes that link the southern and the northern parts of the graph to the central part), whose removal cut the network into significant disconnected parts.

We also measure the value of V_E and $V_{B,1}$, as described in Sect. 4. For the first quantity, we obtained a value of 0.0577 and 0.0084 for Florence's and Attika's PTN, respectively. This means that Florence's network results are more vulnerable than Attika's in terms of decrease of efficiency due to the removal of one single node. However, it is important to remember that Attika has almost eight times the number of nodes of Florence. Then, the damage caused by the removal of a single node is higher in Attika rather than in Florence, in proportion.

For the second quantity, we obtain a value of 0.0022 and 0.0005 for Florence's and Attika's PTN, respectively, coherent with a lower distribution of the number of the shortest paths between the nodes for the Attika's PTN, and the

presence of many links connecting different sub-graphs (i.e. cluster) within the network and having a large value of edge-betweenness.

In conclusion, an a priori analysis of the two PTNs results in a major vulnerability of the Attika's network compared to the Florence's one: the presence of many links towards peripheral regions could cause, in case of an attack to these targets, the disconnection of the network into large disconnected components.

6.2 Simulation of a targeted attack in a static context

To simulate a possible targeted attack in a static context, we simulate the closure of a certain number of the stations/stops, as described in Eq. (15), according to two different lists ordered by:

1. decreasing degree centrality;
2. betweenness centrality.

Such lists were either prepared at the begin of the attack. The results of these attack scenarios are reported in Fig. 6. There, we show changes in S and E for the PTN as a function of the removed nodes fraction c for the above-described attack scenarios. The blue curve and the red curve represent the attacks done using the degree centrality and the betweenness centrality, respectively. The results are shown until the 50% mark of the fraction of the removal nodes.

The more significant decrease of E occurs for the degree curves, which means that a targeted attack has greater success to break up the level of efficiency of the

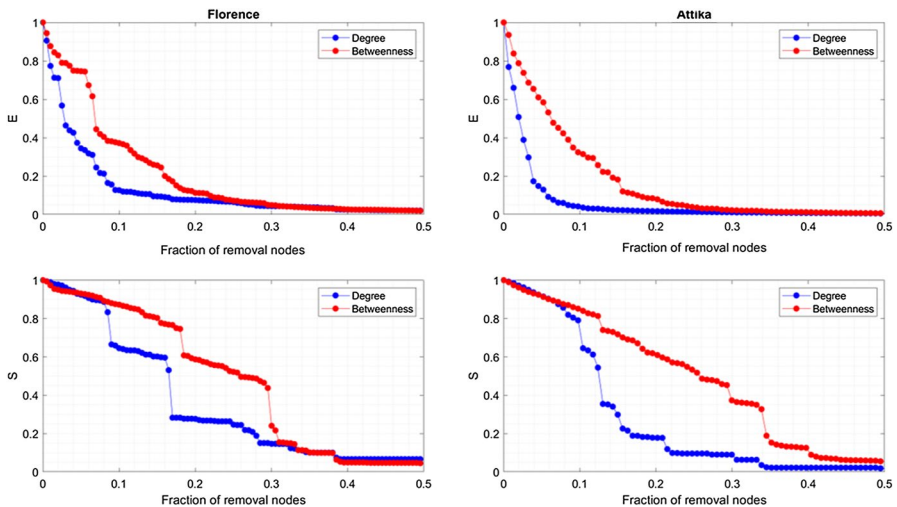


Fig. 6 Changes in E and S for the two PTNs during a possible attack scenario based on a subsequent removal of the nodes according to a list. Each curve corresponds to a different scenario as indicated in the legend. Lists of removed nodes were prepared according to their degree (blue curves), betweenness (red curves), from the highest value to the lowest one, before the beginning of the attack

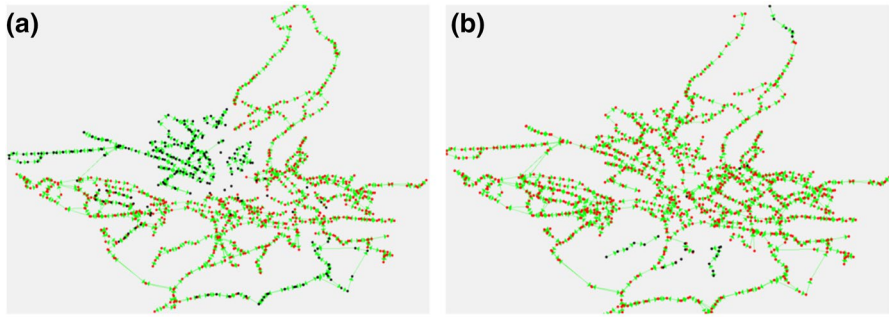


Fig. 7 Graph of Florence's PTN at the end of the targeted attack related to the 0.1 fraction of nodes with **a** highest degree, and **b** with the highest betweenness. The red points indicate the nodes belonging to the largest connected component

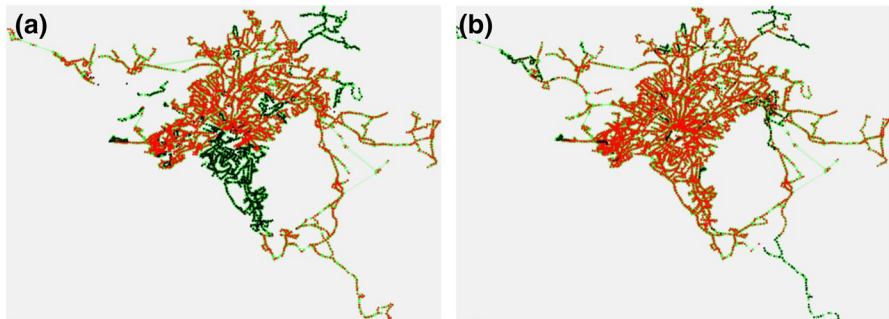


Fig. 8 Graph of Attika's PTN at the end of the targeted attack related to the 0.1 fraction of nodes with **a** highest degree, and **b** with the highest betweenness. The red points indicate the nodes belonging to the largest connected component

network, when the target is the highest degree nodes. In particular, the decrease of E appears to be exponential for both the PTNs and the attacks, and faster for the Attika's PTN compared to the Florence's one.

The behaviour of S appears quite different. In this case, the value of S decreases linearly, but with the presence of different harmful peaks of decrease. For both the attacks, such decrease is very similar until a certain fraction of the removed nodes (about 0.08 for both the PTNs). Then the decrease of degree curves is more significant.

Finally, Figs. 7 and 8 report the resulting graphs of Florence and Attika, respectively, at the end of a targeted attack, which addresses only the 0.1 fraction of the nodes. The red nodes are those belonging to the largest connected component. For both the PTNs, the attacks related to the nodes with the highest degree—Figs. 7b, 8b lead to the creation of new important connected components (high decrease of S). Vice versa, the attacks related to the nodes with the highest betweenness—Figs. 7a and 8a—lead to the removal of many important communication edges (i.e. having a high value of edge-betweenness). This results

in a high increase of the length of the minimal paths between the remained nodes of the graph (decrease of E).

From the results of this test, it is possible to conclude that both the PTNs appear to be more vulnerable to an attack based on the degree centrality rather than an attack based on the betweenness centrality. In particular, the removal of just a small fraction of the nodes (about 0.1) might result in a significant decrease of the efficiency of the PTNs. Both the PTNs appear to be quite resilient to any type of attacks, since the connectivity (S) does not change significantly with respect to its value computed before the attack. When a consistent fraction of the high degree nodes is removed, many large disconnected components appear.

6.3 Simulation of a failure cascade

To simulate a possible capacity cascade for the two networks, we simulate the closure of the station with the highest value of betweenness, as described in Eq. (16). So, we remove this node according to the mechanism described in Sect. 3.2, setting the capacity to $\alpha = 0.01$.

The re-computation of the betweenness for each node permits to identify the new failing nodes in the cascade (i.e. nodes with the capacity lower than the current load). These nodes are removed, and the process iterated until no more nodes fail, as described in Sect. 4.

Figure 9a, b show the two final networks at the end of the cascade, respectively, in which the red points represent the nodes removed from the network. Most of the nodes in both the networks are removed because they exceed their initial capacity. In Florence's PTN most of the removed nodes are localized in the center, near the starting node of the cascade, and in the southern and northern part of the city. Some new edges are created in the graph to maintain the routes, for example, in the northern part of the city. In case of Attika's PTN, even if the starting node of the cascade is localized in one of the external branches, it can be noted that almost all the nodes to be removed are located in the center of the graph, which corresponds to the city of Athens.

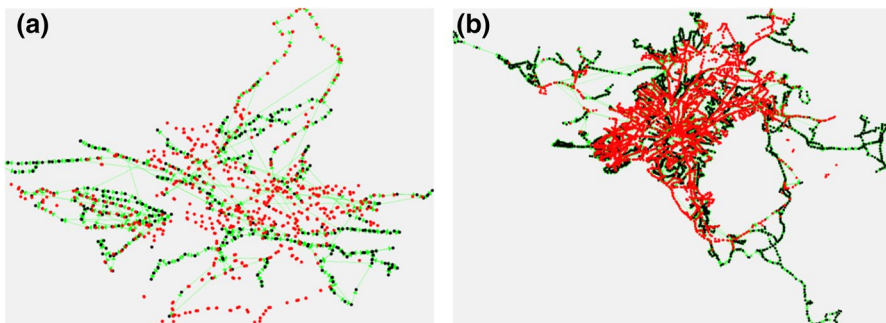


Fig. 9 **a** Graph of the Florence PTN after the cascade effect. **b** Graph of the Attika PTN after the cascade effect. In the figures the red points represent the removal nodes

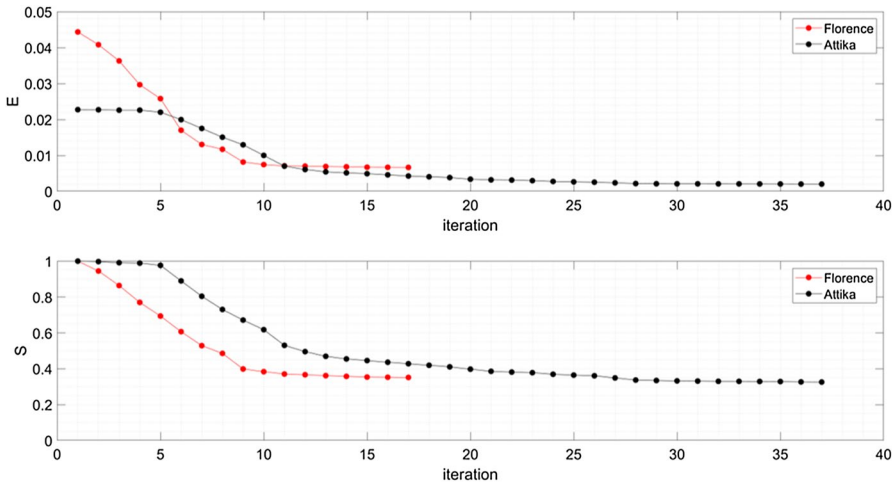


Fig. 10 Values of E (a), S (b) during the cascade. The black curves refer to the Florence PTN. The red curves refer to the Attika PTN

Figure 10 summarizes the values of E and S computed during the cascade. The red and black curves represent the Florence’s PNT, and the Attika’s PTN, respectively.

In the first case (Florence PTN) we note a decrease of the value of S and E , that passes from 1 to 0.35, and from 0.044 to 0.007, respectively, and the length of the cascade is 17. In particular, we note a high decrease of E and S from the 1st to the 10th iteration, followed by a slow decrease until the last iteration. The removal of the starting node causes an important re-distribution of the load at the beginning and the consequent removal of all the nodes exceeding the initial capacity, starting from the center of the city—Fig. 11a—towards the northern and southern part—Fig. 11b. Then, in the second part of the cascade such a re-distribution is lower and only few nodes per iteration are removed.

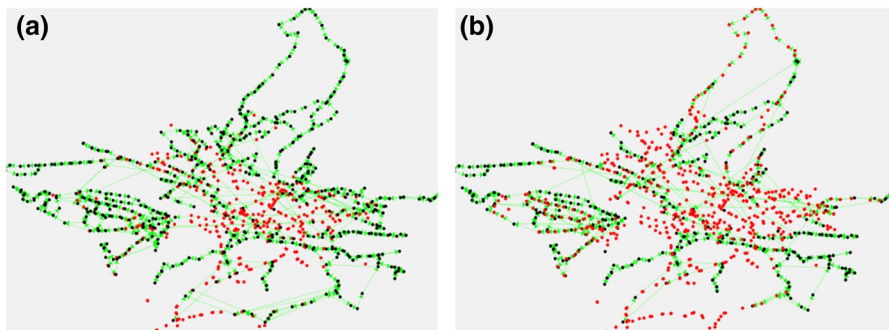


Fig. 11 a Graph of the Florence’s PTN at the 5th iteration of the cascade. b Graph of the Florence’s PTN at the 10th iteration of the cascade. In the figures the red points represent the removed nodes

Also, in the second case (Attika PTN) we note a decrease of the values of S and E , that pass from 1 to 0.32 and from 0.023 to 0.002, respectively, and the length of the cascade is 37. Specifically, a phase with no significant variations of E and S , from the 1st to the 4th iteration, followed by a phase of high decrease from the 5th to the 11th iteration, and by a last phase of low decrease from the 12th until the last iteration of the cascade. Such a diverse behaviour can be explained by the position of the initial node of the cascade. At the beginning, the peripheral position of the node causes only a local redistribution of the load and the removed nodes are few (Fig. 12a). Then, when the cascade propagates toward the centre, the re-distribution of the load and the consequent number of the removed nodes increase (Fig. 12b). Then, in the final part, the cascade propagates towards the other parts of the network, but its effect is minor.

To conclude the analysis, even if the Attika's PTN seems to be more resistant to the cascading effect at the beginning, this is only due to the peripheral position of the starting node. Indeed, at the end of the cascade, after the cascading effect has spread towards the center, the values of E and S of Attika are lower than Florence's ones.

7 Conclusions, results and perspectives

In this paper, graph theory and network analysis are used to model PTN and to analyse their possible vulnerability to a relevant disrupting event, such as the closure/unavailability of one or more of their stations. Such event is considered both in a static and dynamic setting. In the first case, a certain fraction of the nodes is removed subsequently as a function of a list defined a priori according to the degree and the betweenness centrality. In the second case, a cascading failure is triggered starting from the node with the highest betweenness value and all the nodes having a load (re-computed at each iteration of the cascade) exceeding their initial capacity are removed at each iteration of the cascade.

Main studies about attack strategies on public transport are based on a static approach, while in this paper we choose to consider both static and dynamic

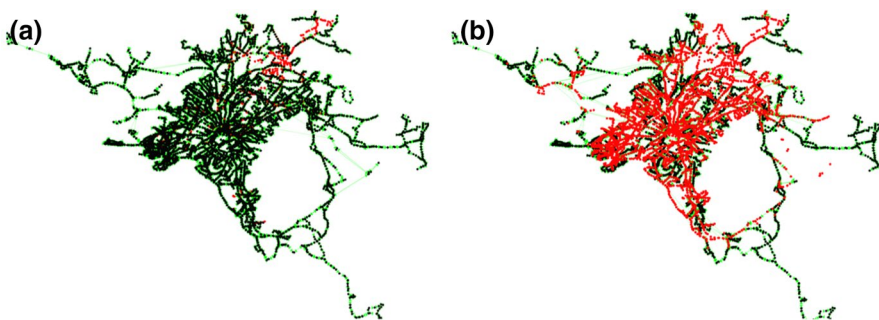


Fig. 12 **a** Graph of the Attika's PTN at the 5th iteration of the cascade. **b** Graph of the Attika's PTN at the 10th iteration of the cascade. The red points represent the removed nodes

approaches to analyse the possible vulnerabilities of a PTN. In addition, the use of the multi-graph approach allowed to have a more significant representation of the PTNs modelling multiple lines/routes between two stations/stops. Besides, maintaining the routes passing through an unavailable station, we simulate a real-transport situation in which, different from the traditional approaches, it is possible to “jump” that station moving from one station to another one on the same line/route.

To analyse the possible modifications in the network, the size of the largest connected component and the efficiency are considered to describe the possible impacts on the whole network. While the first quantity describes how the largest connected component is altered, the second one indicates how efficiently (a.k.a. lengths of minimal paths) the nodes of the network remain connected.

Relevant results obtained on two different and relevant urban environments, the public transport of the city of Florence and the public transport of the Attika’s region, have been presented. Considering the different sizes and forms of the two networks allowed for identifying different characteristics in terms of resilience, vulnerability and efficiency. More important, the proposed analytical framework computes a set of measures in both static and dynamic contexts, proving relevant information on the vulnerability of any PTN with respect to targeted attacks and cascading failures, respectively.

The results allowed to evidence potential vulnerabilities of the urban networks. A targeted attack addressing the highest degree nodes of the network can cause the creation of many connected sub-graphs, disconnected from the largest connected component, whereas an attack addressing the highest betweenness nodes causes the removal of important links of the two networks, with a consequent reduction of efficiency. Furthermore, a cascading failure can cause severe damages to PTNs, both in terms of decrease of the level of E and S . The position of a starting node, in the center of a network (Florence) or in a peripheral position (Attika) is important in terms of velocity of cascade propagation. However, the final level of damage to the PTN can be serious, even in the presence of quite slow cascading effects.

Generally, the planning processes for urban transport focus the attention on the creation of urban networks characterized by high connectivity and interrelation between their components. The results of this paper can support the planning process in the study of possible vulnerabilities of a PTN and in the creation of resilient infrastructures against directed attacks and cascading failures.

Ongoing research is addressing the integration of optimization strategies, from the operative research field, aimed at optimizing the structure of the PTN to improve one or more vulnerability measures.

Regarding targeted attacks, it is possible to analyse which part of the graph implies an important decrease of E and S . This information could be exploited to improve the design of the PTN through the creation of new links and/or stations to avoid the disconnections of the networks into components (decrease of S) and/or as well as the increase of path lengths (decrease of E).

Regarding the cascading failures, it is possible to study which level of tolerance (α) can be useful to avoid new possible failures of the nodes due to their capacity. It is specifically possible to identify which nodes of the PTN are the most important ones to guarantee low impacts of a cascading failure. More precisely, a challenging

optimization goal is the identification of optimal node capacity, under budgetary constraints, to improve the resilience of a PTN.

Acknowledgements This work has been supported by the RESOLUTE project (<http://www.RESOLUTE-eu.org>) and has been funded within the European Commission's H2020 Programme under contract number 653460. This paper expresses the opinions of the authors and not necessarily those of the European Commission. The European Commission is not liable for any use that may be made of the information contained in this paper.

OpenAccess This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

- Agarwal J, Blockley D, Woodman N (2003) Vulnerability of structural systems. *Struct Saf* 25:263–286. [https://doi.org/10.1016/S0167-4730\(02\)00068-1](https://doi.org/10.1016/S0167-4730(02)00068-1)
- Albert R, Barabási AL (2002) Statistical mechanics of complex networks. *Rev Mod Phys* 74:47–97. <https://doi.org/10.1103/RevModPhys.74.47>
- Archetti F, Candelieri A, Giordani I, Arosio G (2015) RESOLUTE PROJECT 2015: application framework
- Ash J, Newth D (2007) Optimizing complex networks for resilience against cascading failure. *Phys A* 380:673–683. <https://doi.org/10.1016/j.physa.2006.12.058>
- Bellini E, Nesi P, Cocone L, et al (2017) Towards resilience operationalization in urban transport system: the RESOLUTE project approach. In: 26th European Safety and Reliability Conference, ESREL 2016, p 345
- Berche B, von Ferber C, Holovatch T, Holovatch Y (2010) Public transport networks under random failure and directed attack. *Dyn Socio Econ Syst* 2:42–54
- Berdica K (2002) An introduction to road vulnerability: what has been done, is done and should be done. *Transp Policy* 9:117–127. [https://doi.org/10.1016/S0967-070X\(02\)00011-2](https://doi.org/10.1016/S0967-070X(02)00011-2)
- Boccaletti S, Buldú J, Criado R et al (2007) Multiscale vulnerability of complex networks. *Chaos*. <https://doi.org/10.1063/1.2801687>
- Bonacich P (1972) Factoring and weighting approaches to status scores and clique identification. *J Math Sociol* 2:113–120. <https://doi.org/10.1080/0022250X.1972.9989806>
- Candelieri A, Soldi D, Archetti F (2015) Network analysis for resilience evaluation in water distribution networks. *Environ Eng Manag J* 14:1261–1270. <https://doi.org/10.30638/eemj.2015.136>
- Cats O, Jenelius E (2015) Planning for the unexpected: the value of reserve capacity for public transport network robustness. *Transport Res Part A Policy Pract* 81:47–61. <https://doi.org/10.1016/j.tra.2015.02.013>
- Cats O, Jenelius E (2018) Beyond a complete failure: the impact of partial capacity degradation on public transport network vulnerability. *Transportmet B* 6:77–96. <https://doi.org/10.1080/21680566.2016.1267596>
- Cats O, Yap M, van Oort N (2016) Exposing the role of exposure: public transport network risk analysis. *Transport Res Part A Policy Pract* 88:1–14. <https://doi.org/10.1016/j.tra.2016.03.015>
- Cohen R, Erez K, Ben-Avraham D, Havlin S (2000) Resilience of the Internet to random breakdowns. *Phys Rev Lett* 85:4626–4628. <https://doi.org/10.1103/PhysRevLett.85.4626>
- Criado R, Romance M (2012) Structural vulnerability and robustness in complex networks: different approaches and relationships between them. In: Springer optimization and its applications, pp 3–36
- Estrada E (2006) Network robustness to targeted attacks. The interplay of expansibility and degree distribution. *Eur Phys J B* 52:563–574. <https://doi.org/10.1140/epjbe2006-00330-7>
- Ferreira P, Simoes A (2015) RESOLUTE PROJECT 2015: conceptual framework

- Freeman LC (1977) A set of measures of centrality based on betweenness. *Sociometry* 40:35. <https://doi.org/10.2307/3033543>
- Gaitanidou E, Tsami M (2016) RESOLUTE PROJECT 2015: ERMG adaptation to UTS
- Gaitanidou E, Bellini E, Ferreira P (2015) RESOLUTE PROJECT 2015: European resilience management guidelines
- Google (2018) Google Transit APIs. In: <https://developers.google.com/transit/>
- Gutfraind A (2012) Optimizing network topology for cascade resilience. In: Thai MT, Pardalos PM (eds) *Handbook of optimization in complex networks*. Springer, New York, pp 37–59
- Holme P, Kim BJ, Yoon CN, Han SK (2002) Attack vulnerability of complex networks. *Phys Rev E Stat Phys Plasmas Fluids Relat Interdiscip Top* 65:14. <https://doi.org/10.1103/PhysRevE.65.056109>
- Jenelius E, Cats O (2015) The value of new public transport links for network robustness and redundancy. *Transportet A Transport Sci* 11:819–835. <https://doi.org/10.1080/23249935.2015.1087232>
- Jenelius E, Mattsson LG (2015) Road network vulnerability analysis: conceptualization, implementation and application. *Comput Environ Urban Syst* 49:136–147. <https://doi.org/10.1016/j.compenvurb.2014.02.003>
- Latora V, Marchiori M (2001) Efficient behavior of small-world networks. *Phys Rev Lett* 87:198701–1–198701–4. <https://doi.org/10.1103/PhysRevLett.87.198701>
- Latora V, Marchiori M (2005) Vulnerability and protection of infrastructure networks. *Phys Rev E Stat Nonlinear Soft Matter Phys* 71:1–4. <https://doi.org/10.1103/PhysRevE.71.015103>
- Latora V, Marchiori M (2007) A measure of centrality based on network efficiency. *N J Phys*. <https://doi.org/10.1088/1367-2630/9/6/188>
- Mattsson LG, Jenelius E (2015) Vulnerability and resilience of transport systems—a discussion of recent research. *Transport Res Part A Policy Pract* 81:16–34. <https://doi.org/10.1016/j.tra.2015.06.002>
- Onnela J-P, Saramaki J, Hyvonen J, et al (2006) Structure and tie strengths in mobile communication networks. <https://doi.org/10.1073/pnas.0610245104>
- Rodríguez-Núñez E, García-Palomares JC (2014) Measuring the vulnerability of public transport networks. *J Transp Geogr* 35:50–63. <https://doi.org/10.1016/j.jtrangeo.2014.01.008>
- Soldi D, Candelieri A, Archetti F (2015) Resilience and vulnerability in urban water distribution networks through network theory and hydraulic simulation. *Procedia Eng* 119:1259–1268. <https://doi.org/10.1016/j.proeng.2015.08.990>
- University de le Havre (2010) GraphStream, a Dynamic Graph Library. <http://graphstream-project.org/>
- Virkar Y, Clauset A (2014) Power-law distributions in binned empirical data. *Ann Appl Stat* 8:89–119. <https://doi.org/10.1214/13-AOAS710>
- Von Ferber C, Holovatch T, Holovatch Y (2009a) Attack vulnerability of public transport networks. *Traffic Granul Flow* 2007:721–731. https://doi.org/10.1007/978-3-540-77074-9_81
- Von Ferber C, Holovatch T, Holovatch Y, Palchykov V (2009b) Public transport networks: empirical analysis and modeling. *Eur Phys J B* 68:261–275. <https://doi.org/10.1140/epjb/e2009-00090-x>
- Zhang X, Miller-Hooks E, Denny K (2015) Assessing the role of network topology in transportation network resilience. *J Transp Geogr* 46:35–45. <https://doi.org/10.1016/j.jtrangeo.2015.05.006>
- Zou Z, Xiao Y, Gao J (2013) Robustness analysis of urban transit network based on complex networks theory. *Kybernetes* 42:383–399. <https://doi.org/10.1108/03684921311323644>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.