Public Transport Networks under Random Failure and Directed Attack

Bertrand Berche[1], Christian von Ferber [2,3], Taras Holovatch [1,2], Yurij Holovatch [4]

[1] Statistical Physics Group, P2M Dpt, Institut Jean Lamour, Nancy Université, BP 70239,
F-54506 Vandœuvre les Nancy, France
berche@lpm.u-nancy.fr
[2] Statistical Physics Group, Applied Mathematics Research Centre, Coventry
University, Coventry CV1 5FB, UK
holovatch@gmail.com
[3] Physikalisches Institut, Universität Freiburg, D-79104 Freiburg, Germany
c.vonferber@coventry.ac.uk
[4] Institute for Condensed Matter Physics, National Acad. Sci. of Ukraine, UA-79011 Lviv,
Ukraine & Institut für Theoretische Physik, Universität Linz, A-4040, Linz, Austria
hol@icmp.lviv.ua

Abstract. The behaviour of complex networks under failure or attack depends strongly on the specific scenario. Of special interest are scale-free networks, which are usually seen as robust under random failure but appear to be especially vulnerable to targeted attacks. In a recent study of public transport networks of 14 major cities of the world we have shown that these systems when represented by appropriate graphs may exhibit scale-free behaviour. In this paper we briefly review some of the recent results about the effects that defunct or removed nodes have on the properties of public transport networks. Simulating different directed attack strategies, we derive vulnerability criteria that result in minimal strategies with high impact on these systems.

1. Introduction

Since the last decade we witness how ideas and methods of graph theory merge with those of statistical physics and give rise to complex network science [1]. The emergence of complex network theory is accompanied by a very fruitful interdisciplinary interaction with different branches of natural and social sciences where some of the present concepts had been originally developed and even in humanities. The fact that many natural and man-made structures have a network topology and in many instances such networks have much in common, allows for a common basis of deeper understanding of different phenomena that occur on such networks and for their quantitative description. The specific type of networks we address in this paper are public transport networks [2-14], that provide an instance of

Dynamics of Socio-Economic Systems, Vol.2 Number 2: 42-54 (2010). ISSN 1852-379x
Received: 17/02/10, Accepted: 20/06/10. http://www.dyses.org.ar/IJ-DySES

the more general class of transportation networks. While for many structures modelled by complex networks the network topology is not immediately apparent and can be recovered only in the course of a thorough analysis of their subtle features, in the case of public transportation the network structure is obvious and it is even fixed in the commonly used term „public transport network“ (PTN). However, as we will see below, there are other, less obvious, options to represent a PTN in the form of a graph [2,4,5,10,15], which results from the fact that its structure is richer than that of a generic complex network. One can discriminate between two main directions of research in the field of complex networks: on the one hand, one is interested in the structural properties of complex networks, on the other hand, one analyzes different phenomena that occur on networks. Our recent analysis of PTN [10-14] shares goals of both of these directions: on the one hand, we analyze topological properties of PTN of 14 major cities of the world [10,11], on the other hand, we address particular processes that may and do occur on PTN [12-13]. Concerning the latter case we analysed effects that defunct or removed nodes have on the properties of PTN. Simulating different directed attack strategies, we derived vulnerability criteria that result in minimal strategies with high impact on these systems. In this paper we briefly review some of our recent results on the behaviour of PTN under random failure or directed attack.

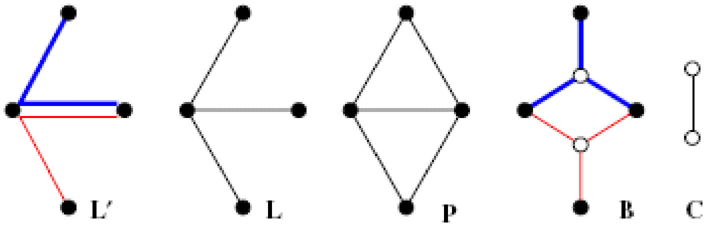

Fig. 1. Representation of a PTN in graph form. **L'**-space: filled circles represent stations serviced by two different routes shown by a bold and a thin line. **L**-space: reduction of **L'** to a simple graph with single links. **P**-space: any two stations that are serviced by a common route are linked. **B**-space: stations (filled circles) are linked to the routes (open circles) they belong to. **C**-space: routes (open circles) are connected when they share a common station

2. PTN representation

The question how the characteristics of a complex network change when some of its constituents are removed has many important practical implementations. Below, we will call such a removal an *attack*. The notion of attack vulnerability of a network originates from studies of computer networks and denotes the decrease of network performance that is caused by removal of its nodes and/or links. In pioneering studies of attack vulnerability of complex networks it was found that their reaction may range from a well-expressed robustness to high vulnerability when the attack scenario is varied [16] . In the case of a PTN, knowledge about its vulnerability allows both to take measures to protect its most vulnerable components as well as to possibly increase its resilience by planning its further development and evolution.

To generate this knowledge we performed a thorough analysis of the behaviour under attack of PTNs of 14 major cities of the world, taking cities from different continents, with different concepts of planning and different history. In our sample, the number of stations N and routes M ranged from $N = 1544$, $M = 124$ (Düsseldorf) to $N = 46244$, $M = 1893$ (Los Angeles). This allowed us to produce a reliable statistics and to access some unique features of the networks under consideration.

There are many different ways to represent a PTN of a city in the form of a graph, some of such representations – 'spaces' - are discussed in Refs. [2,4,5,10,15] and illustrated in *Figs.1,2*. The primary network topology is defined by a set of routes each servicing an ordered series of given stations this may either be interpreted as a multigraph allowing for multiple edges (**L'**-space) or as a simple graph (**L**-space [2,4]), a number of additional neighbourhood relations may be defined both for the routes and the stations. E.g. one can define two stations as neighbours whenever they are serviced by a common route (**P**-space [15]). Further, one may define a bipartite graph (**B**-space) consisting of two classes of nodes: one class representing stations, the other the routes with the obvious relation between routes and stations defining the edges of this bipartite graph. From this one may recover the P-space graph by projection on the station nodes while the complementary projection on route nodes will generate a (**C**-space) graph describing the neighbourhood relations between routes. In the analysis given below we make use of both **L-** and **P-**representations and also give an outlook on how the **B**-space representation may be employed. We will first look into different characteristics of PTN calculated for the corresponding graphs and then analyse attacks and measure how these change these characteristics.

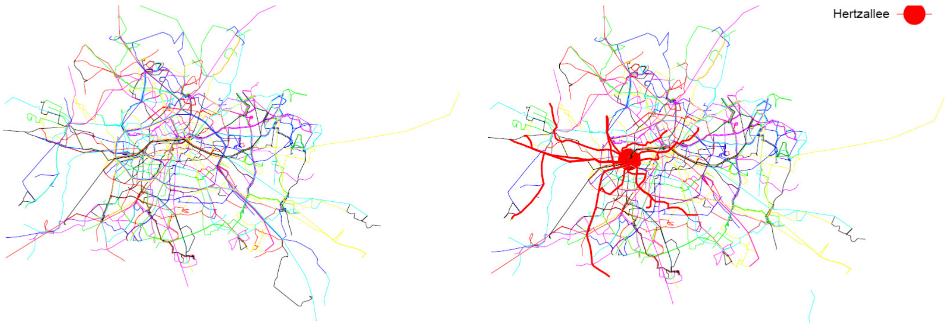

Fig. 2. The PTN of Berlin (left): Interpreting the stations as vertices and the lines as links (identifying multiple edges) results in an **L**-space graph. Right: The sub-network of nodes (links shown in bold red) that can be reached from Hertzallee (shown as a bold red spot) without changing mode of transport corresponds to the **P**-space neighbourhood of that station.

The implementation (and effect) of an attack differs in different spaces: attacks in the **L**-space correspond to situations, in which given public transport stations and all their incident links cease to operate for all means of traffic that go through them, whereas if a station-node is removed in the **P**-space, the corresponding stop of the route is cancelled while the route otherwise keeps operating. The above described attacks refer to the removal of nodes. Alternatively, we have analyzed the behaviour of PTN when the links are removed [14].

With a PTN representation given in the form of a graph we are in the position to describe the observables we will be interested in as well as to describe the way attacks of different strategies are performed.

3. Observables and attack strategies

In practice, the origin of the attack and its scenario may differ to large extent, ranging from random failure, when a node or a link in a network is removed at random to a targeted destruction, when the most influential network constituents are removed according to their operating characteristics [16-18]. Moreover, choosing a certain criterion, one can prepare the list of the nodes for the *initial* network and remove the nodes according to this list. Alternatively, one can continuously measure nodes (or links) characteristics after each step and modify such a list in the course of an attack. Attacks according to recalculated lists often turn out to be more harmful than the attack strategies based on the initial list, suggesting that the network structure changes as important nodes or links are removed [17,19].

One can single out two different impacts to the effectiveness of a network and its resilience during an attack. The first one has purely topological origin and is uniquely defined by network structure, the second one originates from the load on a network (see e.g. [20]), i.e. it takes into account intensity of the transportation processes. In the particular case of a PTN this second impact is characterised by the number of vehicles or number of passengers that use a given route. In our study we will be interested only in the first impact, primary addressing the network topology and leaving aside its load. That is, speaking about network robustness to an attack we will first of all mean how ‘complete’ remains a PTN when its constituents are removed. There are different observables that are usually employed to characterise such robustness. In particular, these are the mean shortest path length $\langle l \rangle$, mean of its inverse $\langle l^{-1} \rangle$, size of the largest component S [12,13,17,21]. Below, we will exploit the last quantity defined as

$$S = N_1 / N, \qquad (1)$$

where N and N_1 are numbers of nodes of the network and of its largest component correspondingly. In practice, for a finite network, such a quantity serves as an analogue of a giant connected component (GCC) which is defined for an infinite network only [1]. In turn, the GCC serves as the analogue of a percolation cluster, when the problem of network resilience is treated in terms of percolation theory [22].

In *Fig. 3* we show how S changes as function of the concentration of removed nodes c when these nodes are removed randomly without any reference to their characteristics. Below, we will call such scenario a random one and denote it as RV (random vertex). The data is displayed for the PTNs of 14 different cities, as listed in the corresponding legends. *Fig. 3a* shows results for the PTN represented as a graph in the **L**-space, whereas *Fig. 3b* shows data for the **P**-space. One immediately notes that the reaction of the **P**-space graphs on random attacks is rather homogeneous and merely corresponds to continuous linear decrease of $S(c)$. This is easy to understand if one recalls that in the **P**-space each route enters the PTN representation as a complete graph and hence a random removal of any station node does not cause network segmentation. On the contrary, the reaction of the PTN graphs on a random attack in the **L**-space ranges from abrupt breakdown (Dallas) to a slow almost linear decrease (Paris).

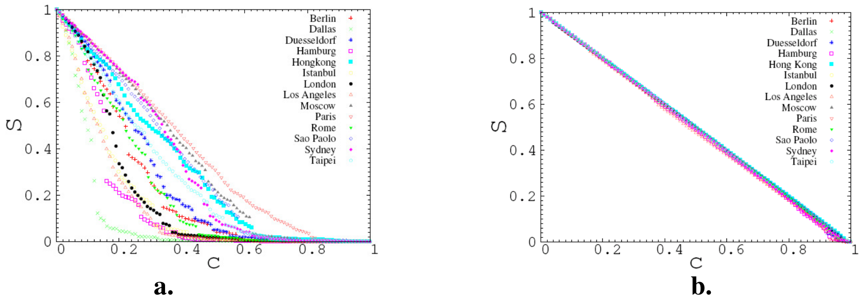

Fig. 3. The largest cluster size S of different PTN as function of the fraction of removed nodes c. Random scenario. **a: L**-space, **b: P**-space

Before discussing correlations between the characteristics of unperturbed PTN and their robustness to attacks let us first explain different attack strategies we pursued in our study. In the network literature different attack scenarios are used to analyse the resilience of a complex network [12-14,17,19]. Generally, these are based on the intuitive assumption that the largest impact on a network is caused by the removal of its most important constituents. To quantify such importance of a node, one often uses the node degree k (i.e. the number of nearest neighbours of a given node), closeness C_C, graph C_G, stress C_S, and betweenness C_B centralities (see e.g. [23] for definitions and discussion). To give an example, for a given node j the last quantity is defined as

$$C_B(j) = \sum_{s \neq j \neq t \in \mathrm{N}} \frac{\sigma_{st}(j)}{\sigma_{st}}, \tag{2}$$

where $\sigma_{st}(j)$ is the number of shortest paths between nodes s and t that belong to the network N and go through the node j.

One can also measure the importance of a given node by the number of its second nearest neighbours z_2 or its clustering coefficient C. The latter is the ratio of the actual number of links between the node's nearest neighbours and the maximal possible number of mutual links between them. In our analysis we made use of different attack scenarios, removing the nodes according to the lists ordered by decreasing node degree k , centralities C_C , C_G , C_S , C_B , number of second nearest neighbours z_2, and increasing clustering coefficient C . Such lists were either prepared for an unperturbed network or recalculated after each step of attack. Together, this makes sixteen different attack scenarios which including the above described random vertex (RV) attack as well as a scenario where a randomly chosen neighbour (RN) of a randomly chosen vertex is removed. The last scenario appears to be effective for immunization problems [24].

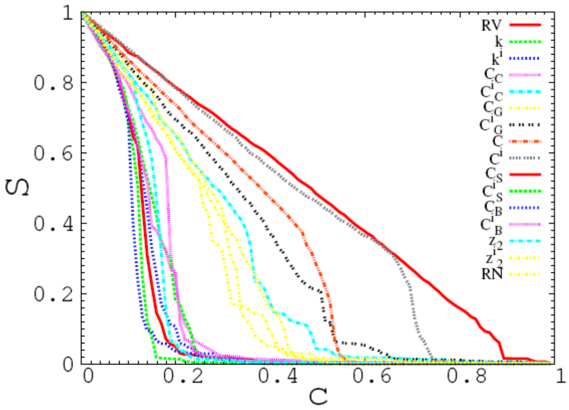

Fig. 4. Largest component size S of the PTN of Paris as function of the fraction c of removed nodes for different attack scenarios. Each curve corresponds to a different scenario as indicated in the legend. Lists of removed nodes were prepared according to their degree k , closeness C_C , graph C_G , stress C_S , and betweenness C_B centralities, clustering coefficient C , and next nearest neighbors number z_2 . A superscript i refers to lists prepared for the initial PTN before the attack. RV and RN denote the removal of a random vertex or of its randomly chosen neighbour, respectively

A typical result of our study is shown in *Fig. 4*. There, we show changes in the largest component size S of the PTN of Paris as a function of the removed nodes fraction c for the above described attack scenarios. Each curve corresponds to a different scenario as indicated in the legend. A similar analysis was performed for all other PTN from our database. As expected, it appears that the impact of an attack for a given PTN graph crucially depends on the attack scenario. Moreover, the most harmful scenarios differ for different graph representations (different 'spaces').

In particular, for the **L**-space graphs the most harmful scenarios are those defined by the node degree, betweenness, closeness and stress centralities, and second nearest neighbours number whereas for the **P**-space graphs the node degree does not play such an important role and the most destructive are centrality-oriented scenarios. In *Fig. 5* we show the size of the largest cluster S of different PTN graphs in **P**-space as a function of the fraction of removed nodes c for the recalculated highest betweenness scenario which appears to be the most destructive for the **P**-space graphs. Indeed, the special role played by the highest betweenness nodes is explained by the fact, that they join different routes (represented in **P**-space by separate complete graphs) and their removal leads to rapid network segmentation.

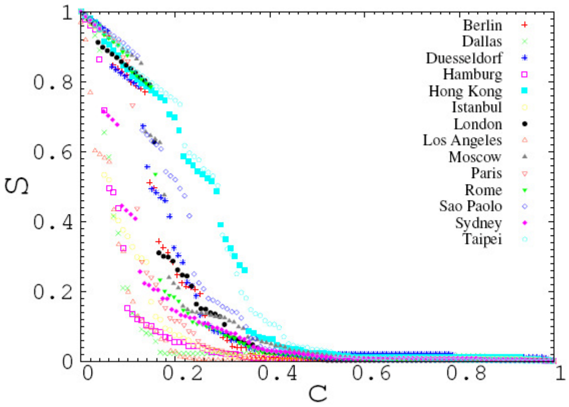

Fig. 5. Size of the largest cluster **S** as a function of the fraction of removed nodes **c. P**-space, highest betweenness scenario (recalculated)

From a statistical physics point of view random attack scenarios may be related to percolation theory. There, it is well established that site and bond percolation on regular lattices show universal behaviour with identical universal exponents, however, as has also been shown for percolation on small world networks [25] the percolation threshold does in general differ between these two scenarios. One may therefore expect similar differences to occur when observing attacks that result in edges being removed. Our research on this question is ongoing [14] and we present a first result in *Fig.6* where the impact of attacks that disable links between node stations in the **L**-space representation is shown for all cities in our sample. For each of the PTN it appears that randomly removing nodes is more effective than randomly removing links. Qualitatively this corresponds to results of [25] where a lower percolation threshold (corresponding to a higher c_s value) was found for bond percolation.

To further investigate the origins of the difference in resilience observed we have looked for correlations between the observed scale-free behaviour of the degree distribution and the resilience against these attack scenarios. In particular, we attempted to fit the node degree distribution to a power-law decay

$$P(k) \sim k^{-\gamma}. \tag{3}$$

With a good fit and in particular a low exponent γ indicating strong scale free behaviour.

In the case of the **L**-space, the scale-free behaviour was markedly observed for 7 PTN out of 14, in the **P**-space these were 4 out of 14. An exponential decay of $P(k)$ observed for the other PTN, nevertheless may be fitted by a power law (3) with less accuracy. Our findings are that strong scale free behaviour, i.e. good fits with small exponents γ is generally correlated with strong resilience, i.e. the network breaking down only at a high segmentation concentration. Notable examples are given by PTN of Paris ($\gamma = 2.62$), Saõ Paolo ($\gamma = 2.72$), and Hong Kong ($\gamma = 2.99$). The segmentation concentration for these PTN at the RV scenario is $c_s = 0.38;0.32;0.30$, respectively. Alternatively, at the same attack scenario PTNs of London ($\gamma = 4.48$), Los Angeles ($\gamma = 4.85$), and Dallas ($\gamma = 5.49$) have much lower segmentation concentration: $c_s = 0.175;0.130;0.090$.

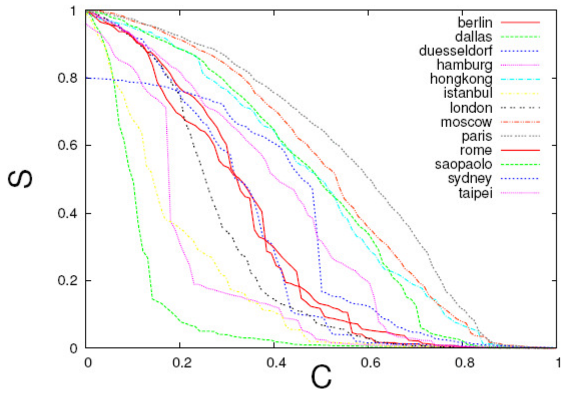

Fig. 6. Testing 'bond percolation': Size of the largest cluster S as a function of the fraction of removed links c. **L**-space, random scenario.

Another instructive observation concerns the applicability of the Molloy-Reed criterion [26] which has been formulated for networks with given node degree distribution but otherwise random linking between vertices. For such equilibrium networks a GCC was shown to be present if

$$\langle k(k-2)\rangle \geq 0, \tag{4}$$

where angular brackets stand for a network average in the limit of an infinite network with given $P(k)$. Therefore, a GCC is absent for small values of the parameter $\kappa \equiv \langle k^2\rangle / \langle k\rangle < 2$. Calculating values of κ for the unperturbed PTN we have found that for these real-world networks smaller values of κ in general indicate a smaller segmentation concentration c_s both for the RV and for the recalculated node-degree attack scenarios in **L**-space.

An analysis of network resilience in **P**-space on the other hand shows that for this particular interpretation of a PTN the mean shortest path length proves to be a useful indicator for PTN robustness. With respect to **P**-space connectivity the path lengths are related to the number of times a passenger needs to switch means of transport. As our detailed analysis [13] shows, short **P**-space path lengths indicate a high resilience of a PTN in the otherwise dangerously effective scenario of attacks on highest betweenness nodes.

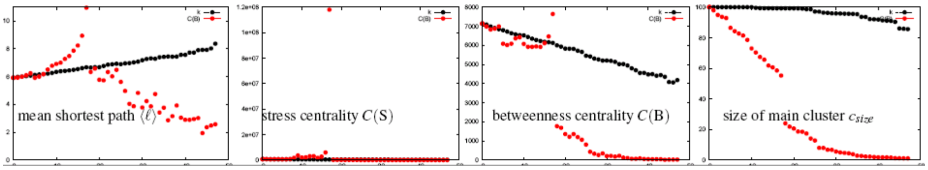

Fig. 7. Search of the segmentation concentration during an attack scenario, here in the case of B-space attacks (see text). From left to right: changes in the mean shortest path length, stress and betweenness centralities and size of the main cluster as functions of C for the highest node degree (black curves) and highest betweenness centrality scenarios for the Berlin PTN Complete breakdown occurs for 18 defunct stations.

To further analyse the way how network resilience may depend on the way the network is interpreted we have recently extended our study to include the bipartite interpretation of PTN graphs called **B**-space, see *Fig. 1* [14]. In this interpretation, both routes and stations are each represented by a distinct class of nodes. In the bipartite graph an edge may only link a node of one class (station) to a node of the other class (route) . Here, each station is linked to all routes servicing it and vice versa. A **B**-space interpretation of an attack on a given station may then be given in the following way: if a given station becomes defunct, then all routes servicing it will be affected and will stop operation or accumulate serious delays sooner or later. For routes operating on tracks this is immediately obvious. Our preliminary findings are that with respect to this realistic interpretation an otherwise seemingly robust network may completely break down with only a few defunct stations. An illustration is given for the Berlin PTN in *Fig. 7* where a number of network indicators are monitored as function of the number of defunct stations. We find that the size of the largest component decreases rapidly with a technical breakdown with only 18 defunct stations. Obviously, from an operational viewpoint a breakdown would be declared even earlier. In a real world scenario this explains how e.g. in the case of industrial action a small group of transport union activists may enforce a breakdown by blocking only a selection a handful of stations.

4. Conclusions and outlook

Public transport networks (PTNs) though sharing many of the known features of other complex networks have a particularly rich structure due to their underlying multilayer nature. The basic layer of roads or tracks (invisible in our data), on top of that the **L**-space of all roads and tracks that are in use by the routes and further on top of these the layer of routes. Both inside and in-between layers different networks can be found in terms of graphs defined by node-edge relations starting either from a geographical approach (**L**-space) or a relational one (**B**-space that offers different projections.)

In our analysis we attempt to identify correlations between the characteristics of the unperturbed PTNs and their robustness to attacks. In particular, we exploit the fact [10], that some of the PTNs under consideration manifest scale-free properties. Analysing this in more detail, we found that fitting the degree distribution to a power law decay allowed us to classify this behaviour in the following way: a network is scale free in a 'strong' sense if the fit is good and the resulting exponent small, otherwise the scale free behaviour is weak or absent. Our analysis has revealed significant correlations between the numerical value of the node-degree distribution exponent γ and the segmentation concentration of PTN (the last was numerically estimated on the base of different methods in [12,13], see also *Figs. 6,7* for illustration). Our findings show that strong scale free behaviour with a small value of γ corresponds to high robustness against various attack scenarios in particular for both for the RV and the recalculated node-degree attack scenarios in **L**-space.

Making use of a general criterion for the appearance of a giant connected component within equilibrium networks we established that the respective 'Molloy-Reed' parameter calculated for the unperturbed network may be employed as an estimator of network resilience.

Comparing with results from exact percolation studies on small-world networks [25] we find qualitative agreement with a prediction that bond percolation displays lower percolation thresholds that site percolation.

We have further seen that using other graph interpretations of PTNs leads to additional insight into their resilience as a function of their architecture. For the **P**-space interpretation which focuses on the number of changes between means of transport we have found that short **P**-space paths generally indicate a high resilience of these networks. Particularly striking results are revealed when analysing the bipartite graph of the **B**-space interpretation. Here, we found explanations for the effective breakdown of such networks already at very low numbers of defunct stations.

The properties and characteristics of the various representations that we have discussed here make this field of PTN research richer than other known complex networks. However, we believe that some of the methods and ideas developed here may also be useful in other contexts.

Acknowledgements

The paper is based on an invited lecture given by one of us (Yu.H.) at the Workshop „NET 2009: evolution and complexity" (Rome, May 28th-30th, 2009). The hospitality of the organizers is kindly acknowledged. This work was supported by the following institutions and projects: Austrian Fonds zur Förderung der wissenschaftlichen Forschung under Project No. P19583-N20 (Yu.H.), cooperation programme 'Dnipro' between the Ministry of Foreign Affairs of France and the Ministry of Education and Science of Ukraine (B.B. & Yu.H); Ecole Doctorale EMMA of the University Nancy and an Overseas Research Student Scholarship (T.H.), and the Applied Research Fellow Scheme of Coventry University (CvF).

References

[1]. R. Albert, A.-L. Barabási, *Statistical mechanics of complex networks*. Rev. Mod. Phys. **74**, 47, (2002; S. N. Dorogovtsev, J. F. F. Mendes, *Evolution of networks* . Adv. Phys. **51,** 1079, (2002); M. E. J. Newman, *The Structure and Function of Complex Networks*. SIAM Review **45,** 167, (2003); S. N. Dorogovtsev, S. N. Mendes, *Evolution of Networks.* Oxford University Press, Oxford, 2003.

.

[2].V. Latora, M. Marchiori, *Is the Boston subway a small-world network?* Physica A **314**, 109, (2002).

[3].K. S. Kim, L. Benguigui, M. Marinov, *The fractal structure of Seoul's public transportation system*. Cities **20**, 31, (2003).

[4].K. A. Seaton, L. M. Hackett, *Stations, trains and small-world networks*. Physica A **339**, 635, (2004).

[5].J. Sienkiewicz, J. A. Hołyst, *Statistical analysis of 22 public transport networks in Poland*. Phys. Rev. E **72**, 046127, (2005); J. Sienkiewicz, J. A. Hołyst, *Public transport systems in Poland: from Białystok to Zielona Góra by bus and tram using universal statistics of complex networks.* Acta Phys. Pol. B **36**, 1771, (2005).

[6].P.-P. Zhang, K. Chen, Y. He, T. Zhou, B.-B. Su, Y. Jin, H. Chang, Y.-P. Zhou, L.-C. Sun, B.-H. Wang, D.-R. He, *Model and empirical study on some collaboration networks.* Physica A **360**, 599, (2006).

[7].X. Xu, J. Hu, F. Liu, L. Liu*, Scaling and correlations in three bus-transport networks of China*. Physica A **374,** 441, (2007).

[8].M.-B. Hu, R. Jiang, Y.-H. Wu, W.-X. Wang, Q.-S. Wu, *Urban traffic from the perspective of dual graph*. Eur. Phys. J. B **63**, 127, (2008).

[9].Zhu Z.-T. Zhu, J. Zhou, P. Li, X.-G. Chen, *An evolutionary model of urban bus transport network based on B-space.* Chinese Physics B **17**, 2874, (2008).

[10].C. von Ferber, Yu.Holovatch, V.Palchykov, *Scaling in public transport networks*. Condens. Matter Phys. **8**, 225, (2005); C. von Ferber, T. Holovatch, Yu. Holovatch, V. Palchykov, *Network harness: Metropolis public transport*. Physica A **380**, 585, (2007); C. von Ferber, T. Holovatch, Yu. Holovatch, V. Palchykov, *Public transport networks: empirical analysis and modeling*. Eur. Phys. J. B **68**, 261, (2009); C. von Ferber, T. Holovatch, Yu. Holovatch, V. Palchykov, *Modeling Metropolis Public Transport*. In: C. Appert-Rolland, F. Chevoir, P. Gondret, S. Lassarre, J.-P. Lebacque, M. Schreckenberg (Eds.) Traffic and Granular Flow '07. Springer, 2009, 709.

[11].B. Berche, C. von Ferber, T. Holovatch, *Network harness: bundles of routes in public transport networks*. In: B. Berche, N. Bogolyubov, Jr., R. Folk, and Yu. Holovatch (Eds.), Statistical Physics: Modern Trends and Applications. AIP Conference Proceedings **1198,** Melville, New York (2009) 3.

[12]. C. von Ferber, T. Holovatch, and Yu. Holovatch, *Attack vulnerability of public transport networks.* In: C. Appert-Rolland, F. Chevoir, P. Gondret, S. Lassarre, J.-P. Lebacque, M. Schreckenberg (Eds.) Traffic and Granular Flow '07. Springer, 2009, 721.

[13].B. Berche, C. von Ferber, T. Holovatch, Yu. Holovatch*, Resilience of public transport networks against attacks*. Eur. Phys. J. B **71**, 125, (2009).

[14].B. Berche, C. von Ferber, T. Holovatch, *unpublished.*

[15].P. Sen, S. Dasgupta, A. Chatterjee, P. A. Sreeram, G. Mukherjee, S. S. Manna*, Small-world properties of the Indian railway network.* Phys. Rev. E **67,** 036106, (2003).

[16]. R. Albert, H. Jeong, A.-L. Barabàsi, *Error and attack tolerance of complex networks*. Nature **406**, 378, (2000). R. Cohen, K. Erez, D. ben-Avraham, S. Havlin*, Resilience of the internet to random breakdowns.* Phys. Rev. Lett. **85**, 4626, (2000). D. S. Callaway, M. E. J. Newman, S. H. Strogatz, D. J. Watts, *Network robustness and fragility: percolation on random graphs*. Phys. Rev. Lett. **85**, 5468, (2000). R. Cohen, K. Erez, D. ben-Avraham, S. Havlin, *Breakdown of the internet under intentional attack*. Phys. Rev. Lett. **86**, 3682, (2001).

[17]. P. Holme, B. J. Kim, C. N. Yoon, S. K. Han, *Attack vulnerability of complex networks*. Phys. Rev. E **65**, 056109, (2002).

[18]. L. K. Gallos, P. Argyrakis, A. Bunde, R. Cohen, S. Havlin, *Tolerance of scale-free networks: from friendly to intentional attack strategies*. Physica A **344**, 504, (2004); L. K. Gallos, R. Cohen, P. Argyrakis, A. Bunde, S. Havlin, *Stability and topology of scale-free networks under attack and defence strategies*. Phys Rev. Lett. **94**, 188701, (2005).

[19]. M. Girvan, M. E. J. Newman, *Community structure in social and biological networks,* Proc. Natl. Acad. Sci. USA **99**, 7821, (2002).

[20]. A. E. Motter, Y.-C. Lai, *Cascade-based attacks on complex networks*. Phys. Rev. E **66,** 065102(R), (2002).

[21]. P. Crucitti, V. Latora, M. Marchiori, A. Rapisarda, *Efficiency of scale-free networks: error and attack tolerance*. Physica A **320**, 622, (2003).

[22]. D. Stauffer, A. Aharony. *Introduction to Percolation Theory.* Taylor & Francis, London, 1991.

[23]. U. Brandes, *A Faster Algorithm for Betweenness Centrality*, J. Math. Sociology **25**, 163, (2001).

[24]. R. Cohen, S. Havlin, D. ben-Avraham, *Efficient immunization strategies for computer networks and populations,* Phys. Rev. Lett. **91**, 247901, (2003).

[25]. C. Moore, M. E J. Newman, *Exact solution of site and bond percolation on small-world networks,* Phys. Rev. E **62**, 7059, (2000).

[26]. M. Molloy, B. A. Reed, *A critical point for random graphs with a given degree sequence,* Random Struct. Algorithms **6**, 161, (1995).