Revisiting Models of Vulnerabilities of the Networks

Horia-Nicolai L. TEODORESCU

Romanian Academy, Iasi Branch,
Bd. Carol I nr. 8, Iasi, Romania,
hteodor@etti.tuiasi.ro

Abstract: The study critically revisits the models of 'vulnerability' of various types of networks and shows several limits of the current state of the art, including the ambiguous definitions of vulnerability and robustness concepts, the arbitrary use of various connectivity indexes on graphs for assessing the 'vulnerability' of real-world networks to real-world attacks, the lack of any evidence for the proposed models, and the lack of significant statistical approaches. Next, the study shows the limits of using the world 'measure' and 'metric' in relation with connectivity characteristics on graphs. Then, a general cause-effect chain for attacks on networks, especially computer and transportation networks is laid down as a basis for probabilistic model building. Evidence is provided on the relation between graph features and the probabilities of events under an attack and model examples are discussed. An annex on the caution of making public detailed knowledge on such models ends the paper.

Keywords: networks, attacks, risk, connectivity indexes, network vulnerability, probabilistic model, evidence.

1. Introduction

For more than four decades, the issues of the reliability and vulnerability to attacks were studied for computer and communication networks (CCN), mainly using graph models and tools [4], [5], [25], [29]. More recently, similar tools have been applied to transportation systems in relation with several infamous attacks in various countries [8], [19]. A large number of studies have been recently devoted to the vulnerability of transportation networks [19], especially of subways [7], [9-11], [32], [33] due to several attacks on them. Many of these studies focused on the vulnerability of nodes and edges of the networks, in relation with the network topology, and proposed indexes of vulnerability, sometimes weighted by flows; in this way, the models for computer networks were directly transposed to transportation ones, without discussing the foundation of the model extension from one type of networks to another. These studies have no evidence support and remain largely disconnected from the real life situations; moreover, many of these studies use intuitive yet qualitative and vague meanings for features such as vulnerability, robustness, and resilience.

We critically revisit some of the concepts and issues related to 'vulnerability' and concerning specifically transportation networks; new network indexes are proposed that have the potential of being more suitable (Section 4). Next, probabilistic models are suggested for the attacks and for computing the outcome in probabilistic terms for attacks, depending on the node properties (Sections 3-5).

The first set of contributions of this study is theoretical; in obtaining them, the method applied is based on graph analysis and probabilistic approach; tentative speculative models are proposed (Sections 3-5). A second core contribution consists in binging evidence for the derivation of models for key probabilities involved in the analysis; examples are presented and references to actual transportation networks are made in Section 6. The remaining part of this introductory section is devoted to the terminology related to graph features and to the general concept of vulnerability.

The organization of the paper is largely linear; Section 2 reviews some graph models related to vulnerability of networks, while Section 3 and 4 clarify aspects related to chains of effects and the related probabilities. Section 5 details the role of nodes and edges in the attack probability of networks. A model based on seemingly natural assumption is built in Section 6 and its predictions are contrasted in Section 7 with the evidence-based models for attack probability. The last section contains conclusions.

2. Graph Models and Vulnerability Indices

There is a large number of graph "measures" usable for assessing the complexity of and for characterizing the structure of networks, see a subset of them explained in [3], [13], [14], [16],

[18], [21], [23], [30], [31]. Many of these parameters relate to the connectivity degree of graphs, or on the centrality of the nodes; others are based on statistical foundations, such as entropy and Fisher information [1]. In this paper we avoid the name of "measure" because some of the definitions of the involved parameters do not satisfy the requirements of the definition of distance (thus, they are not metrics) and do not satisfy the defining conditions for (sub-) additive measures. Recall that a distance d is a two variable, positive-valued real function; the distance between two object x and y is defined by the properties (i) $d(x,x)=0$; (ii) $d(x,y)=d(y,x)$; (iii) $d(x,z)\le d(x,y)+d(y,z)$ (Archimedean distance). Also, a measure is a set-variable, positive real valued function μ that has the properties: (i) $\mu(\varnothing)=0$; (ii) is (sub-)additive, that is, for any countable set of disjoint sets, A_k, $\mu(\cup_k A_k)\le\sum_k \mu(A_k)$; (iii) it is defined on a σ-algebra, meaning that the measure is defined on complements of sets and on any countable union or joint of measurable sets. Some of the "graph measures" used in the literature refer strictly to a single node or edge, but reflect its relation with the rest of the graph, and are thus far from any type of measure or metric currently accepted.

For example, the degree of a vertex $v\in V$ in a graph $G=(V,E)$ is not a measure or a metric at it refers to a single vertex, it is a topological feature representing the vertex vicinity and connectedness; however, the absolute value of the difference between the degrees of two nodes is a distance. On the other hand, the diameter of a graph is based on the distance between nodes, defined as the minimum number of edges from one node to the other, when all paths and all couples of nodes are considered . When joining two graphs, the diameter of the new graph is less or equal to the sum of the diameters of two of its subgraphs (plus 1 for the joining edge), thus satisfying (sub-)additivity. Yet, the diameter of the graph is not a distance, as there is no such thing as the diameter of the couple (G,G) to determine if the property (i) above holds. The use of the confusing term "measure" in relation to graphs probably comes from the use of the parameters in assessing (quantifying) the vulnerability of a network, or just its connectedness. For avoiding confusions and improper use of terms, we will use "index", following [25] and others, in connection with the reliability of computer and transportation networks; this term is better suited.

Another misleading issue is that virtually all studies relate the 'vulnerability' of networks solely to the connectivity properties of the corresponding graphs. The resilience, vulnerability etc., cannot depend only on the topology of the network; it also depends on the duration of recovery and the type of the attacks and on their probabilities. The destruction of a bomb attack followed by fire is much larger and requires much longer time of investigation plus recovery, than an attack with a gun. Also, several types of attacks have to be taken into account, each with its own probability. Moreover, the architecture and structural elements of the stations and their vulnerabilities affect the overall vulnerability and must be taken into account.

Compared to previous approaches, this one ours is essentially statistical. In the first place, a distinctive feature of the approach is that the probability of the attack at a specified node depends on the structural (topological) properties of the network. Next, several types of attacks are considered. Fourth, the damage and recovery times for various nodes is assigned as a function of the node structural and material (physical) realization. The probability of the propagation of the attack is also considered. Next, probabilistic models are proposed for the attacks and their consequences.

One of the limits of previous graph models of transportation networks such as railway and bus networks is that they do not fully account for the terminal stations; in fact, each „final" node has the possibility to turn the trains the other way around; therefore, these nodes are defined by self-loops. Notice that, according to this definition, final nodes do not necessarily correspond to the final (end) stations in a transportation network; stations along the path may have self-loops. Also notice that in case of transportation networks where trains can travel in both senses (either having engines at both ends, or having the ability to drive backwards), the concept of self-loop is not required – all the stations may be considered as having self-loops. Self-loops on the 'internal' nodes, standing for the ability to drive in both directions, significantly increase the reliability of the system, compared to the case of trains

with a single driving direction ability, as they allow for independent operation on isolated subgraphs, provided that any isolated path has a self-loop – again, an issue not clarified by previous studies.

We will differentiate, along with Hernandez, and Mieghem [18] between the class of topological (structural) metrics and the class of service metrics. On the other hand, we depart from their definition of resilience, which is in fact a (inexplicit) definition of robustness, "*The project* ([34]) *defines resilience as the ability of a network to provide and maintain an acceptable level of service in the face of faults to normal operation*." These authors also tend to make no distinction between robustness and reliability, "reliability has been the classical way to quantify network robustness" (p. 10, [34]).

Most studies in the field have been preoccupied with the refinement of the so-called "measures" or "metrics" related to the connectivity of nodes in graphs, with few dealing with elements of the cause-effect relationship. Moreover, we were not able to find studies relating evidence to the significance of the connectivity indexes, which is a curious situation. The approach in this study starts with the analysis of the causal chains and next deal with evidence related to elements of the causal chains.

3. Cause-Effect Chains of Attacks

The discussion in this study follows the diagram in Figure 1, which presents the general frame of the cause-effect chains in an event. The attacked target may be a transportation network, indiscriminate choice of human groups, etc. In a specified transportation network, the target can be a station, a line, or a train. We assume that a transportation system is the target; then, in Figure 1, the attack target is restricted to stations, lines, and trains.

Example. For computer and communication networks (CCNs), the attack target can be a data center, or a communication line, or the system(s) of a specific (group of) user(s), e.g., users of fitness or health devices. When the target is a server or a datacenter, the choice can be made based on the centrality degree of it, for example its data flow level, or its degree as a vertex in the network. Once the minimal degree is chosen, the attacker will make a specific choice of the network element randomly or based on other considerations. Next, the attacker makes a choice of the type of attack, for example among using spam to lure a user in giving access, using malware infected sticks, or monitoring and finding patterns in the traffic, or searching faults in the encoding etc.

4. Probabilities

The probability that an attack occurs on a network, p_a, has to be estimated by experts, based on the overall political and social situation in the respective country and on the regional or global contexts. This probability is known to be highly dependent on time, as the above mentioned contexts may fast change. The conditional probability that, if an attack happens, it is of type $t \in \{vertex, edge(line), carrier\}$ is denoted by $p_t = p(t|a)$. This probability should be estimated based on evidence; the topic is discussed in Section 6.

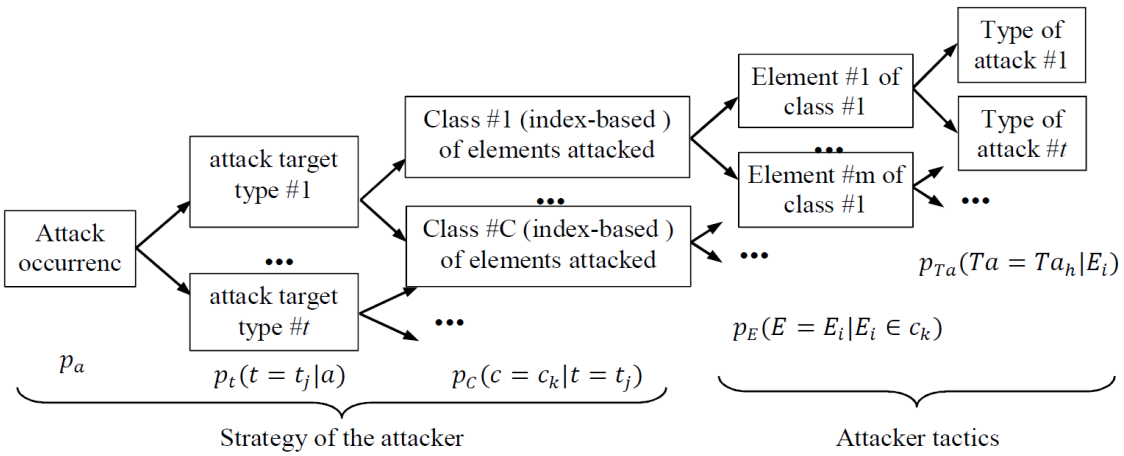

Figure 1. Cause-effect potential chains and decision tree of an attack

The probability p_t depends on several factors, such as time (epoch) and country. The epoch determines what kind of hacker or other attacker groups are active and on their representations and tactics.

The probability of the attack of type t being successful is denoted by $p_{ats}=p(a=success|t)\,p(t|a)\,p(a)$. Next, the probability that the attacked element of the network of the specified type (vertex, edge, or carrier) belongs to a specified subclass is to be estimated based on evidence and on the knowledge of the tactics of the potential attackers. Here, the subclass may be characterized by the degree of the vertices, by their centrality, or by the flow on the edge. This topic is discussed in Sections 4 and 5. The probability that a specified element of the network is attacked is then determined on the structure of the network; for example, if the network includes m elements in the given class (e.g., m vertices with the same degree *d*), the probability of choosing any of those elements is $1/m$. Further, the resulted degree of damage to the network and consequently the time of recovery differ according to a probability distribution that depends on the class of elements as above discussed and on the characteristics of the specified element, for example the structural characteristics of the attacked station and its capacity to withstand explosions.

The overall risk of the network at a given moment is finally computed as the sum of the risks of its elements, where the risk of an element of being attacked and the average time of recovery of the network are determined as explained above.

5. Dissecting the Role of Nodes and Edges from the Point of View of the Attacks

The application domain and goal of the analysis dictate the choice of measures of the network that should be used. A communication network and a spreading of infections are applications that significantly differ; in addition, the interests in robustness and in reliability are significantly different as aims of the calculations. Therefore, for every application and targeted property, another choice of measures is probably recommended. As explained by Piraveenan et al. [23], "*it is not always likely that contagion will spread along shortest paths in networks. Indeed, pathological infection is more likely to spread randomly, where a person who is a 'contact' to an infected person is vulnerable to infection with a certain probability.*"

An irrational attacker may choose the target randomly, attacking with uniform (i.e., the same) probability any node or edge of the network. In that case, the (statistical) structural properties and flow properties of the graph are applicable for determining what the effect of the attack may be. For example, in this case, we should be concerned about the probability that a node or edge breaks the network into subnetworks, about how many such disconnected graphs appear, and about what is the decrease in the flux through the network and what costs produces that decrease. Notice that rational attackers may also act in this way, when trying to avoid countermeasures likely protecting the most critical nodes and edges, or when trying to confuse the attacked and to create most panic and psychological effects (disbelief, uncertainty). Also, the attacker may wish to produce the maximal structural, flow, or cost damage. In this case, a rational attacker would strike in the nodes that produce most structural disconnection in the network, respectively the highest financial loss.

If only structural (topological) damage is the concern, indices of damage must be first chosen. Such indices may be the number of disconnected graphs produced and the number of nodes disconnected from the remaining largest subgraph. Subsequently, we will use these indicators.

The topology of the graph may be regarded as composed of three main "elementary" blocks: "stars", "loops" (rings) and "whiskers", the last being strings of at least two vertices, all 2-degree, except the terminal ones, connected one to the other.

Stars are simply nodes with at least two edges; they are important because of their interconnection role. Nodes connected only to a star become detached by cutting a single edge. When two stars are connected, they form multiple paths between their neighbors, see Figure 2. Loops are important because they may bind together stars and whiskers and create alternative paths between non-adjacent nodes.

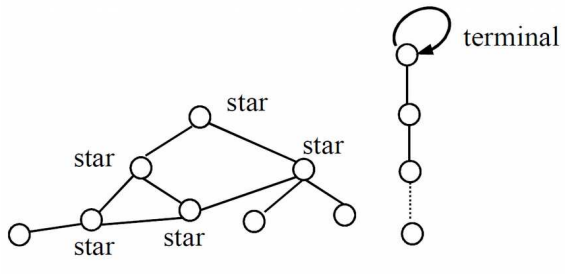

Figure 2. Stars and terminal node in a graph

At least two edges must be broken or two nodes deleted to disconnect the loop. When there are multiple imbricate loops, the structure is more difficult to disconnect. Smaller are the loops, smaller is the probability that one of their edges or nodes is damaged by a random attack on the graph. Loops improve the connectivity stability between distant nodes allowing for more paths between them.

'Whiskers', which will be named isolated paths, are strings of nodes and edges that connect only between themselves, each node having at most two neighbors. They are 'vulnerable' because a single node removed produces a disconnected graph.

The ratio $\rho_1=\frac{n_{star}}{|V|}$, where n_{star} is the number of stars in the graph, may be a good indicator of the connectedness strength of the graph. Also, the ratio $\rho_2=\frac{n_{loop}}{|V|}$ is an indicator of the connectivity of the graph. Therefore, ratios such as $\frac{\rho_1+\rho_2}{2}=\frac{n_{star}+n_{loop}}{2|V|}$ and $\sqrt{\rho_1^2+\rho_2^2}$ can be used as compact connectedness strength indicators. Instead, $\rho_3=\frac{n_{whisker}}{|V|}$, where $n_{whisker}$ is the number of nodes in whiskers, shows the level of weakness in connection. Again, one may wish to compress the three in a single index, for example as $\rho_4=\frac{\rho_1+\rho_2}{2}-\rho_3$, with networks with negative values of ρ_4 being highly sensitive to disconnection by attacks.

Example. Bucharest metro has six stars (Basarab, Piata Victoriei, N. Grigorescu, Dristor, P. Unirii, and Eroilor) and the largest vertex degree is 4. It has a single loop and six whiskers. The number of vertices is 4 on the green line (stations on two lines are counted once; here Gara de Nord and Basarab are not counted), one on the black line (Republica-Pantelimon), 12 (exclusively) on the blue line, 8 (exclusively) on the red line, and 20 on the yellow line that also forms a loop. Therefore, $|V|=45$, $\rho_1=\frac{6}{45}$, $\rho_2=\frac{1}{45}$, and $\rho_3=\frac{6}{45}$. Notice that ρ_4 has a negative value, $\rho_4=-\frac{2}{15}$.

As shown in Section 6, evidence indicates that stars are the main attack targets; empirical data do not indicate a specific interest for the loops. As a final remark, whiskers are frequent on transportation networks and were frequent on old telephony networks, but they are almost missing from current computer networks; therefore, ρ_3 is not significant for the latter ones.

6. Models for Attack, Costs and Resilience

Subsequently, we refine the relation of the connectivity indexes with the attack probability calculations. First, we need to state the problem, namely, to decide if the interest is in the computation of the robustness, of the resilience, or of whatever feature of the network is of interest. Next, we have to specify the assumed strategy that the attacker will adopt. We assume that the strategy is "attack the node that is the most important topologically". We need to adopt one of several reasonable models for the parameters of the robustness or resilience; there are several definitions and approaches for that, for example [2], [15], [20], [22], [26-28], [34], to name but a few. The model should be completed by including definitions of the involved probabilities, of the factors the parameters depend on, on the losses, and the models that connect the probabilities and losses to various factors.

The probability of attack of a node n may increase (for example, linearly or exponentially) with the γ power of the connectivity degree of a node, up to a constant that is network-specific:

$$p_a(n=v)=A_N e^{-\frac{1}{a_N}\left(\frac{1}{c(v)}-\mu\right)^{\gamma}}$$

where N stands for the graph of the respective network, v for the specified node, c is a measure of connectivity or a measure of

centrality of the nodes, and a_N is another parameter of the network. The model is based on the unverified assumption that the more connected or central nodes are, the more compelling they are for attack, because the gain to cost ratio is the highest for them. In addition, another assumption specific to this model is that the attack likeliness (attractiveness) increases exponentially with the centrality index. Both hypotheses remain to be proved or rejected. This general exponential model includes the Gauss distribution with average μ and other exponential distributions, including the typical exponential one, $p(x)=A\,e^{-\frac{x}{a}}$.

Notice that the cost of the attacker is multidimensional and consists of the number of lives lost and the cost for training, equipment used and lost, etc. Also, one may assume that the cost is roughly proportional to the number of attackers. The gain of the attackers is equal to the loss of the attacked entity and includes loss of lives, damage or loss of facilities, costs of the subsequent investigation, cost of rescue operation (for law enforcing forces, rescue entities, medical system), operational losses until the attacked system fully resumes operation, loss of prestige and related future customers, etc. The essence of the success of hacker terrorist group is due to the high ratios gain vs. costs, both in monetary and in life costs, whenever the attacked is ill prepared.

An alternative speculative model is that the node is more probable of being attacked according to a linear law,

$$p_a(n=v)=A_N c\left(\frac{v}{a_N}\right)$$

where the factor A_N includes a normalization factor. One can further speculate that another model is based on the traffic through the nodes; specifically, the probability of attack of a node n increases with the traffic Θ_n in that node; specifically, the increase is with the power θ of the traffic, $p_a(n)=A\,e^{\frac{\Theta_n^\theta}{b}}$. With this model, the cost of the attack of type a_i is

$$\langle C(n,a_i)\rangle=\left\langle \sum_n^{\square} p_{a_i}(n)\,p_{a_i=s}(a_i)\,p_{a_i}(a_i,\Lambda)\right\rangle$$

$$\langle C(n,a_i)\rangle=\left\langle A\,e^{\frac{\Theta_n^\theta}{b}} A_N\,e^{-\frac{1}{a_N}\left(\frac{1}{c(v)}-\mu\right)^\gamma} p_{a_i=s}(a_i,n)\,p_{a_i}(a_i,\Lambda)\times\Lambda\right\rangle$$

The product $p_{a_i=s}(a_i)\,p_{a_i}(a_i,\Lambda)$ can be estimated by attack prevention exercises and tests on scaled down models of the network. Assuming that the attacks are of small, discrete number of categories, for a specified couple (n,a_i), $A\,e^{\frac{\Theta_n^\theta}{b}} A_N e^{-\frac{1}{a_N}\left(\frac{1}{c(v)}-\mu\right)^\gamma}$ and the probability of success in the node n, $p_{a_i=s}(a_i,n)$, are constants. Therefore, the average cost for the node n is

$$\langle C(n,a_i)\rangle=A\,e^{\frac{\Theta_n^\theta}{b}} A_N e^{-\frac{1}{a_N}\left(\frac{1}{c(v)}-\mu\right)^\gamma} p_{a_i=s}(a_i,n)\times \times\int_0^\Lambda \Lambda\cdot p_{a_i}(a_i,\Lambda)\,d\Lambda.$$

Notice that the cost Λ represents the overall cost for the network (and the entity at large), not the cost of destruction at the node site.

However, the above tentative models, which look reasonable for both transportation and communication networks, are only a guess, which proves to be only partly correct, as shown in the next section.

7. Evidence-based models for the probability of attack of vertices as a function of graph indexes

Attacks on computer networks and transportation systems are not new and not restricted to a specific country or continent. A compilation of data in 2010 (at [35]) indicates that most attacks occur in Pakistan, India, Iraq, Turkey and Israel, Columbia. Interestingly, the evidence comes mainly from non-official and non-scientific sources, such as media and public compilations of the data from media, such as Wikipedia. This is due to the lack of technical details publication by the local or national authorities that investigated the respective attacks and to the lack of reporting scientists during the time and at the scene of the investigations. The data show that Europe, particularly Italy, France and UK in the 1970s and 1980s, Russia and France in the 1990s, the 2000s, and the 2010s have seen frequent attacks on trains and subways.

For providing a minimum insight on the probabilities, based on evidence, we collected the data since 1960 on the attacks on the rail and subway transportation systems around the world. The fortunately few data do not offer a sound statistical basis for deriving conclusions;

therefore, the results in this Section should be used with high reservations.

The statistics compiled leads to the distribution of attacked stations in relation with the vertex degree as shown in Figure 3. Notice that we used only the degree of nodes attacked as parameter of the probability, but after dividing the vertex degree to the maximal degree in the graph; in this way, we obtained a single range $[0,1]$ for the relative degrees, making them comparable across different graphs. To fit the data, several models have been attempted, including linear, polynomial, and logarithmic ones, but with limited success. The model based on polynomial regression is

$$p(d) \approx -0.5\,d^2 + 3.5\,d - 2$$

with $R^2 = 1$ (the third power of d was neglected, as it has a very small multiplicative constant). The obtained logarithmic model (based on log regression, using log link function) is

$$p(d) \approx 2.292 \ln d + 1.179$$

with $R^2 = 9.49$. The logarithmic model seems better justified than the polynomial one. At this level of rough analysis, there is little reason to use more intricate vertex indexes, because the vertex degree index already provides a high R^2 value ($R^2 = 0.95$ for the logarithmic model and $R^2 = 1$ for the polynomial model). In consequence, we are justified to argue that the extant statistic data makes futile the theorizing on complicated and computationally time-consuming indexes such as centrality, betweeness, and aggregated indexes.

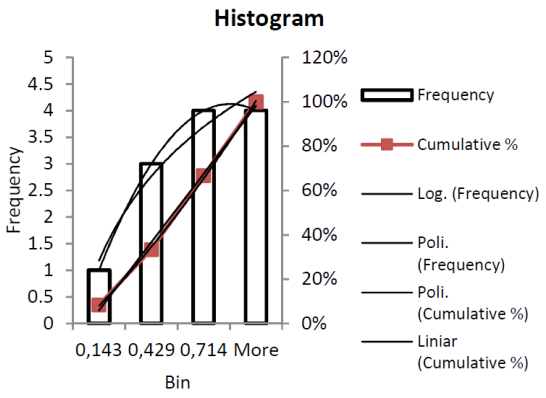

Figure 3. Empirical probability distribution and approximations

On the other hand, running a regression on the cumulative function, one obtains

$$p_C(d) \approx 0.0208\,d^2 + 0.2042\,d - 0.1458$$

with the value of the coefficient of goodness of fit (coefficient of determination) $R^2 = 0.9993$, which makes the second or third order approximation of $p(d)$ less credible.

The finer grained histogram in Figure 4 shows that the linear and logarithmic models are wrong; a high order polynomial (6^{th} degree) performs acceptably ($R^2 = 0.88$), but this has little meaning.

The approximation of the distribution of vertex degrees for attacked stations, with histogram forced to six intervals (fine grained) was attempted with polynomials of various orders. The best fit was obtained with $R^2 = 0.84$ for the fifth degree polynomial

$$p(d) = 0.0212\,d^5 - 0.3876\,d^4 + 2.6129\,d^3 - \\ - 8.059\,d^2 + 11.329\,d - 4.8058.$$

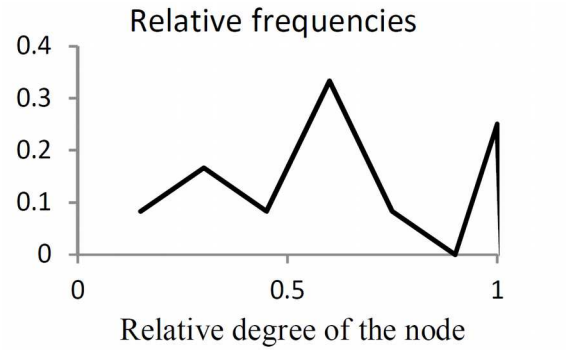

Figure 4. Relative frequencies of the vertex degree of the stations related to attacks (1970-2016), in a forced finer grain histogram. The horizontal axis is the relative degree of the node, that is, the degree of the attacked node vs. the maximum degree of a node in the respective network.

For avoiding approximation errors and rechecking the logarithmic model (which may have some intuitive support), the absolute frequencies have been added to 1 (for evading $\log 0$) and then the logarithms were computed. The results were tested for linear regression, which is obtained as having the slope 0, in agreement with a possible log model, but the value of R^2 is almost 0. Again, the closest approximation is a polynomial with large degree (four), but the value of R^2 is poor. This result is justified by the shape of the histogram in Figure 4; in fact, Figure 4 point toward a mixture of two distributions, with an easy to find interpretation. Further details and a viable

model can be obtained from the author, see the ending note. Interestingly, we found no case when whiskers are attacked; instead, stars of degree 3-8 have been attacked in all cases. Based on this remark, we believe that the index ρ_1 is worth studying in the future; also, the above observation indicate that networks with a large number of stars are more difficult to protect, although they are also more difficult to disable.

8. Conclusions

This paper argued in the first place for a consistent use of the concept of attack probability and risk, based on sound probabilistic approaches. A causal analysis produced the splitting of the overall probability determination process into a number of causal steps and the related conditional probabilities. The estimation of some of these probabilities, such as the one of the attack and the conditional probability of type of attack remain based in on estimation by experts. Some other probabilities, such as the one that the attack produces a certain level of damage to the building (station) or equipment (e.g., lines) can be determined by specialized computations and experiments.

Many remarks exposed in Sections 2-5 are valid for both transportation and communication networks. The fortunate lack of statistics makes difficult to check theoretical models of specific types of attack, or in relation to the type of vertex and edges. Consequently, playing with sophisticated models and vertex indexes remains an instructive, but of little use academic exercise. An interesting future research topic is to determine attack probabilities for large sections of the networks, after it was decomposed into key parts using one of the known effective algorithms, such as [17]. A more complex analysis than the one reported here is possible, but we feel that it is undesirable to publish it. Complete information on this study is kept available for interested parties.

Acknowledgements

The partial support of the SPS-NATO grant G4877 for this research and its publication is acknowledged. Also acknowledged is the support of a DAAD research grant for a visit at Universität der Bundeswehr München and thus for facilitating stimulating discussions with Prof. S.W. Pickl and with M.S. Nistor, to whom thanks are addressed. Also thanks to Mr. M.S. Nistor and anonymous referees for useful suggestions of improvements of the text.

REFERENCES

1. AHMAD, N., S. DERRIBLE, T. EASON, H. CABEZAS, **Using Fisher Information in Big Data**. https://arxiv.org/ftp/arxiv/papers/1507/1507.00389.pdf. (Oct. 5, 2016).
2. ANTHONY, K. R. N., J. M. DAMBACHER, R. BEEDEN, **A Framework for Understanding Cumulative Impacts, Supporting Environmental Decisions and Informing Resilience-Based Management of the Great Barrier Reef World Heritage Area**. Commonwealth of Australia 2013. Publisher Great Barrier Reef Marine Park Authority 2013. https://www.environment.gov.au/system/files/resources/2910cf7e-30fc-466f-a6c1-0e27aa618d05/files/framework-resilience-based-management_0.pdf. (Oct. 5, 2016)
3. BORGATTI, S. P., **Centrality and Network Flow**. Social Networks vol. 27, (2005), pp. 55-71.
4. BOESCH, F., R. THOMAS, **On Graphs of Invulnerable Communication Nets**. IEEE Transactions on Circuit Theory, 1970, Vol. 17, 2, pp. 183-192.
5. BOESCH, F. T., **A Survey and Introduction to Network Reliability Theory**. ICC '88, IEEE Int. Conf. Digital Technology - Spanning the Universe, 1988, vol. 2, pp. 678-682.
6. BOESCH, F., A. FELZER, **On the Minimum *m* Degree Vulnerability Criterion**. IEEE Trans. Circuit Theory, 1971, Vol., 18, 2, pp. 224-228.
7. CHOPRA, S. S., T. DILLON, M. M. BILEC, V. KHANNA, **A Network-Based Framework for Assessing Infrastructure Resilience: A Case Study of the London Metro System.** J. The Royal Society Interface, Vol. 13, 118, 2016 (p.20160113) Doi 10.1098/rsif.2016.0113, (accessed Oct. 5, 2016).

8. DEHMER, M., M. S. NISTOR, W. SCHMITZ, AND K. A. NEUBECKER, **Aspects of Quantitative Analysis of Transportation Networks**. Future Security 2015, Berlin, Sept. 2015, pp. 239-244.

9. DERRIBLE, S., **Network Centrality of Metro Systems**. PLoS ONE vol. 7, 7: e40575. doi:10.1371/journal.pone.0040575, 2012, (accessed Oct. 5, 2016).

10. DERRIBLE, S., N. AHMAD, **Network-Based and Binless Frequency Analyses**. PLoS ONE 10(11): e0142108. doi:10.1371/journal.pone.0142108., 2015 (accessed Oct. 5, 2016).

11. DERRIBLE, S., C. KENNEDY, **The Complexity and Robustness of Metro Networks**. Physica A: Statistical Mechanics and its Applications, Vol. 389, 17, 1 Sep 2010, pp. 3678-3691.

12. DONNINGER, C., **The Distribution of Centrality in Social Networks**. Social Networks, vol. 8 (1986), pp. 191-203.

13. DUCRUET, C., J.-P. RODRIGUE, **Graph Theory: Measures and Indices**. https://people.hofstra.edu/geotrans/eng/methods/ch1m3en.html (acc. Oct. 5, 2016).

14. ESTRADA, E., D. J. HIGHAM, N. HATANO, **Communicability Betweenness in Complex Networks**. https://arxiv.org/ftp/arxiv/papers/0905/0905.4102.pdf. (accessed Oct. 5, 2016).

15. EZELL, B. C., S. P. BENNETT, D. VON WINTERFELDT, J. SOKOLOWSKI, A. J. COLLINS, **Probabilistic Risk Analysis and Terrorism Risk**. Risk Analysis, Vol. 30, No. 4, 2010.

16. FREEMAN, L. C., **Centrality in Social Networks Conceptual Clarification**. Social Networks, vol. 1, 3, (1978), pp. 215-239.

17. HABIB, M., F. DE MONTGOLFIER, C. PAUL, **A Simple Linear-Time Modular Decomposition Algorithm for Graphs, Using Order Extension.** In T. Hagerup, J. Katajainen (Eds.) 9th Scandinavian Workshop on Algorithm Theory, 2004, Humlebaek, Denmark. Springer, pp.187-198, 2004, LNCS vol. 3111.

18. HERNANDEZ, J. M., P. van MIEGHEM, **Classification of Graph Metrics**. www.nas.ewi.tudelft.nl/people/Piet/papers/TUDreport20111111_MetricList.pdf (acc. Oct. 5, 2016).

19. KERMANSHAH, A., S. DERRIBLE, **A Geographical and Multi-Criteria Vulnerability Assessment of Transportation Networks against Extreme Earthquakes**. Reliability Engineering & System Safety, Vol. 153, Sep 2016, pp. 39-49.

20. KLINKE, A., O. RENN, **A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies**. Risk Analysis, Vol. 22, No. 6, 2002.

21. LI, C., Q. LI, P. VAN MIEGHEM, H. E. STANLEY, H. WANG, **Correlation between Centrality Metrics and their Application to the Opinion Model**. http://arxiv.org/pdf/1409.6033.pdf 2014. (accessed Oct. 2, 2016).

22. LINKOV, I., et al., **Changing the Resilience Paradigm**. Nature Climate Change, vol. 4, 2014, pp. 407-409.

23. PIRAVEENAN, M., M. PROKOPENKO, L. HOSSAIN, **Percolation Centrality: Quantifying Graph-Theoretic Impact of Nodes during Percolation in Networks**. PLoS ONE, vol. 8, 1 (2013): e53095. doi:10.1371/journal.pone.0053095 (acc. Oct. 1, 2016).

24. SAREWITZ, D., R. PIELKE, JR., M. KEYKHAH, **Vulnerability and Risk: Some Thoughts from a Political and Policy Perspective**. Risk Analysis, Vol. 23, No. 4, 2003.

25. SOI, I. M., K. K. AGGARWAL, **Reliability Indices for Topological Design of Computer Communication Networks.** IEEE Trans. Reliability, Vol. R-30, 5, Dec. 1981, pp. 438-443.

26. TEODORESCU, H.-N., **Defining Resilience using Probabilistic Event Trees**, Environment Systems and Decisions, 2015, Vol. 35, 2, pp. 279-290.

27. TEODORESCU H.-N. L., S. W. PICKL, **Properties and Use of a Resilience Index in Disaster Preparation and Response**. 2016 IEEE Int. Symp. Technologies for Homeland Security, May 10-12 Waltham, MA USA.

28. TEODORESCU H.-N., S. W. PICKL, **Computing and Optimizing the Index of Resilience of Networks and Information Systems**. Romanian J. Information Science and Technology, vol. 19, Nos. 1-2, 2016, pp. 116-126.

29. TEODORESCU, H.-N., A. KIRSCHENBAUM, S. COJOCARU, & C. BRUDERLEIN (Eds.), **Improving Disaster Resilience and Mitigation- IT Means and Tools**. NATO Science for Peace and Security Series - C: Environmental Security, no. 1874-6519, 2014, Springer, New York, Ch. 1.

30. TIZGHADAM, A., A. LEON-GARCIA, **Betweenness Centrality and Resistance Distance in Communication Networks**. IEEE Network, Nov/Dec 2010, pp. 10-16.

31. WANG, H., J. M. HERNANDEZ, P. VAN MIEGHEM, **Betweenness Centrality in a Weighted Network**. Physical Review E 77, 046105 2008.

32. ZENIL, H., S. DERRIBLE, **World Metro Networks,** Wolfram Demonstration Project http://demonstrations.wolfram.com/World MetroNetworks/ (accessed Oct. 2, 2016), Published: Jan 29, 2014 http://demonstrations.wolfram.com/.

33. YIN, H., B. HAN, D. LI, Y. WANG. **Evaluating Disruption in Rail Transit Network: A Case Study of Beijing Subway**. Procedia Engineering, Vol. 137, 2016, pp. 49-58.

34. *** **ResumeNet**, European Union Research Framework Programme 7, FP - 224619 http://www.resumenet.eu/] (acc. Oct. 5, 2016).

35. *** https://en.wikipedia.org/wiki/List_of_terrorist_incidents_in_2010 (accessed Oct. 5, 2016).