

Transport and Telecommunication, 2012, Volume 13, No 4, 255–260
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia
 DOI 10.2478/v10244-012-0020-x

FAILURE DEVELOPMENT IN A SYSTEM OF TWO CONNECTED NETWORKS

Ilya B. Gertsbakh¹, Yoseph Shpungin²

¹*Department of Mathematics, Ben-Gurion University
 P. O. Box 653, Beer-Sheva, 84105, Israel
 E-mail: elyager@bezeqint.net*

²*Software Engineering Department
 Sami Shamoon College of Engineering, Beer Sheva, 84100, Israel
 E-mail: yosefs@sce.ac.il*

We consider a pair of networks A and B which are subject to failures of their components. In A , edges are subject to failure, and A fails when it disintegrates into several isolated clusters each containing a single terminal. Edges of A fail in random order and their failure moments follow Poisson process. After A has failed, terminal α of A causes a failure ("attacks") on R_α randomly chosen non terminal nodes of network B . All edges incident to an attacked node are erased. The "attacks" take negligible time. Network B failure takes place if it loses its terminal connectivity. We study the probability that B will be in failure state at moment t as a function of t and $R = \sum R_\alpha$. The main formal tools which we use are the D-spectra (signatures) of networks A and B and de Moivre's combinatorial formula.

Keywords: *Network terminal connectivity, signature, D-spectrum, Poisson process, Monte Carlo, random allocation, de Moivre formula*

1. Introduction

Networks attract overgrowing interest in modern research literature. Since network type systems presently appear in every sphere of our life (social networks, communication networks, Internet, etc.) their reliability, survivability and resilience studies are becoming a hot and important issue. Particular interest is attracted by the so-called cascading failure phenomena in networks, i.e. massive network failures triggered by failure of a small part of the network components; see e.g. [7] and many references presented there on this issue.

Majority of the works on network reliability deals with probabilistic failure description and modelling in a single network. At the same time most modern networks do not exist and function in an isolated mode. As noted in [2], "due to technological progress, modern systems are becoming more and more coupled together. While in the past many networks would provide their functionality independently, modern systems depend on one another to provide proper functionality". For example, the financial network of banks and related financial institutions is interconnected with the business network of industrial enterprises. A "failure" (e.g. bankruptcy) of a particular bank in one country may cause serious problems of financing and/or industrial activity of several enterprises operating in another part of the world.

One of the few works devoted to the failures in interdependent networks is an important paper [2], which discusses as an example a communication network and the power supply network. In this case, the nodes of the communication network, which control the operation of power supply stations, depend on the power supplied by the power station, while the power station operation depends on information and control supplied by the communication network.

In the work [2] is considered cascade-type phenomena in a pair of networks having different topology and equal number of nodes, which interact with each other on the basis of one-to-one correspondence between the nodes of both networks: if a node α of network A becomes dysfunctional, then the same happens with its image node of $\beta = \beta(\alpha)$ of B . Initially, a $(1 - p)$ fraction of nodes in A become nonfunctional. This means that all edges in A incident to these nodes are erased. Simultaneously, the "images" of failed A -nodes, also become nonfunctional and the B -edges incident to them are also erased. As a result, both networks disintegrate into a number of isolated clusters. The problem investigated in [2] is the following: "what is the critical $p = p_c$ below which all the mutual clusters constitute only an infinitesimal fraction of the network, i.e. no mutual giant component exist".

In this paper we study a pair of small networks A and B with different topologies. Several nodes in A (called *terminals*) "mark" (or "attack") in a random and independent way a certain number of non terminal nodes in B . Similarly to [2], all edges incident to a marked (attacked) node $\beta \in B$ are erased.

Typically, we will consider edge failures in network A , as a result of which it disintegrates into a number of isolated clusters. (A cluster is a connected isolated sub network containing at least one terminal).

The first phase of the process of failure development in our model is disintegration of A into isolated clusters resulting from a random process of its edge failures that is governed by a Poisson process. After this phase ends, all terminal nodes of A "mark" ("attack") in a random way some number of non terminal nodes in B . It means the beginning of the second phase of network failure. All edges incident to marked (attacked) nodes of B are erased, as a result of which B may be in failure state, according to its operational criterion. For example, B may lose its $s-t$ connectivity. We assume that the second stage lasts negligible amount of time. The problem which we investigate is the following. Assume that at $t=0$ network A starts to disintegrate. Then we are interested in finding the probability $P(DOWN_B; t)$ that network B will be in failure state at moment t .

The further exposition is as follows. In section 2 we consider the formal model of networks A and B and the failure development mechanism. Section 3 is devoted to the derivation of the expression for $P(DOWN_B; t)$. Section 4 presents a numerical example of two small networks. A has 25 nodes, 34 edges and 4 terminals and B has 20 nodes, including 3 terminal nodes, and 34 edges. Failure of B is the loss of terminal connectivity. After A fails each of its terminals "attacks" 3–5 non terminal nodes of B . We investigate numerically how $P(DOWN_B; t)$ depends on t and the total number of "attacks".

2. Model Description

Network A. Network A is a triple $N_A = (V_A, E_A, T_A)$, where V_A is the set of nodes (vertices), $|V_A| = n_A$; E_A is the set of edges (links), $|E_A| = m_A$, and T_A is a subset of special nodes called *terminals*, $|T_A| = r_A$. Edges in A are subject to failures, edge failure means that the edge is erased. Edges fail in random order according to a Poisson process having rate λ . In other words, random intervals between edge failures have exponential distribution with density $f(t) = \lambda \exp(-\lambda t)$. The probability that exactly x failures take place in the interval $[0, t]$ equals therefore

$$P(N(t) = x) = (\lambda t)^x \exp[-\lambda t] / x!, x = 0, 1, 2, \dots \quad (1)$$

In the course of edge failures, A disintegrates into separate components, where each component is a connected sub network isolated from other sub networks. An isolated connected sub network, which contains a terminal, is called *cluster*.

Initially, A is connected and has therefore a single cluster. When edges fail, the network disintegrates into several clusters. The state when N_A falls apart into r_A clusters means, by the definition, the failure of A denoted as $DOWN_A$ -state.

Network B. B is a triple $N_B = (V_B, E_B, T_B)$, where V_B is the set of nodes, $|V_B| = n_B$; E_B is the set of edges (links), $|E_B| = m_B$ and $T_B \subset V_B$ a set of special nodes called terminals, $|T_B| = r_B$. The components subject to failure in this network are the *nonterminal nodes*. Node β failure means that all edges incident to it are erased, and therefore β becomes isolated. The $DOWN_B$ state is defined in terms of terminal connectivity, e.g. as loss of $s-t$ connectivity, or isolation of one of the terminals from other terminals, see e.g. [3, 4, 5]. Another option is defining the $DOWN_B$ state as network disintegration into connected isolated subnetworks the largest of which does not have more than L_{\max} nodes [6].

Action of A on B. Each terminal $i \in T_A$ is randomly mapped onto M_i non terminal nodes in B , which means the following. M_i nodes of B are randomly and equiprobably chosen from the set of $n_B - r_B = n_0$ nodes. One can imagine this mapping as a sequential process of random throwing of M_i balls into n_0 boxes. (It is not excluded that two or more balls may fall into the same box).

One can imagine that M_1 balls are randomly thrown from terminal 1 of A into n_0 white boxes. All boxes receiving at least one ball are coloured red. Then the same procedure takes place for the second terminal, and M_2 balls again are randomly and independently thrown into the same n_0 boxes. The white boxes which receive a ball are coloured red. The red boxes receiving again a ball remain red, and so on, until the procedure is repeated $r = |T_A|$ times. Denote by $R = M_1 + \dots + M_r$ the total number of balls thrown into the n_0 boxes. In another language, one can say that each A -terminal "attacks" a random number of non terminal nodes in B , see Figure 1.

Let us denote by $p_k(R; n_0)$ the probability that exactly k boxes will be red. The following de Moivre's formula (see [1], p. 242) gives this probability:

$$p_k(R; n_0) = \binom{n_0}{k} \sum_{t=0}^k \binom{k}{t} (-1)^t \left(\frac{k-t}{n_0} \right)^R. \tag{2}$$

Let us assume that the action of A on B is implemented in the following way. After network A gets *DOWN*, its terminals randomly "throw balls" on the non terminal nodes of B in the above described manner. This "bombardment" lasts negligible time.

The nodes of B receiving a ball (marked "red") are declared as failed, and all edges incident to these nodes are erased. As the result, B may get *DOWN*. Our ultimate goal is to find the probability $P(DOWN_B; t)$ that B is *DOWN* at moment t .

Remark: cascading failures. According to *WIKIPEDIA*, "cascading failure is a failure in a system of interconnected parts in which the failure of a part can trigger the failure of successive parts". In our system of two networks, the cascading effect will exist if complete isolation of few terminals in A causes network B to enter $DOWN_B$ state.

3. Probabilistic Analysis

The central role in our analysis is played by the so-called network D-spectra [3, 4]. Let us shortly remind this notion. Suppose that we number the network components subject to failure as 1, 2, ..., n . Consider a random permutation $\pi = \{i_1, i_2, \dots, i_n\}$ of these numbers. Assign to each permutation probability $1/n!$. Imagine that all components are functional ("up") and we start turning them down moving along the permutation from left to right. After each step of this process we check the state of the network and note the number of the components needed to be turned down to reveal for the first time that the network has failed.

Let

$$P(\text{the network failed on step } j) = f_j, j = 1, 2, \dots, n. \tag{3}$$

Obviously, $\{f_j\}$ is a proper discrete density: $\sum_{j=1}^n f_j = 1$. In literature it is known also under the name *signature* [8]. We will use the *cumulative signature* (*cumulative spectrum*) $F(x)$ defined as

$$F(x) = f_1 + f_2 + \dots + f_x, x = 1, 2, \dots, n. \tag{4}$$

The probabilistic meaning of $F(x)$ is the following: $F(x)$ is the probability that the network is *DOWN* if exactly x of its randomly chosen components are *down*.

In practice, the exact computation of $F(x)$ is an NP-complex problem, and usually it is approximately calculated using Monte Carlo, see [3, 4].

Now suppose that we know the D-spectra $F_A(x), x = 1, \dots, m_A$, and $F_B(y), y = 1, 2, \dots, n_0$ of networks A and B , respectively. (We remind that there are m_A edges subject to failure in A and n_0 nodes subject to failure in B).

Let us find the probability $P(DOWN_A; t)$ that A will be *DOWN* at the instant t . Obviously,

$$P(DOWN_A; t) = \sum_{x=1}^{m_A} (\lambda t)^x \frac{e^{-\lambda t}}{x!} F_A(x) + \sum_{x>m_A} (\lambda t)^x \frac{e^{-\lambda t}}{x!} . \tag{5}$$

(The second sum in (5) is the probability that there will be more than m_A failures in $[0, t]$ which leads to network failure with probability 1).

After A has failed, as a result of the second phase, some random number of nodes Y in B will be damaged. We know the distribution of Y , see (2):

$$P(Y = k) = p_k(R; n_0), k = 1, 2, \dots, \min(n_0, R).$$

Given that k nodes in B are damaged, B is *DOWN* with probability $F_B(k)$. This gives the following probability that B is *DOWN* if A is *DOWN*:

$$P(DOWN_B | DOWN_A) = \sum_{k=1}^{n_0} P(Y = k) \cdot F_B(k) . \tag{6}$$

Finally, we are ready to write the expression for the probability $P(DOWN_B; t)$:

$$P(DOWN_B; t) = P(DOWN_A; t) \cdot \sum_{k=1}^{n_0} P(Y = k) \cdot F_B(k) . \tag{7}$$

4. Example

Network A has 25 nodes, 34 edges and $|T_A| = r = 4$ terminals, see Figure 1a.

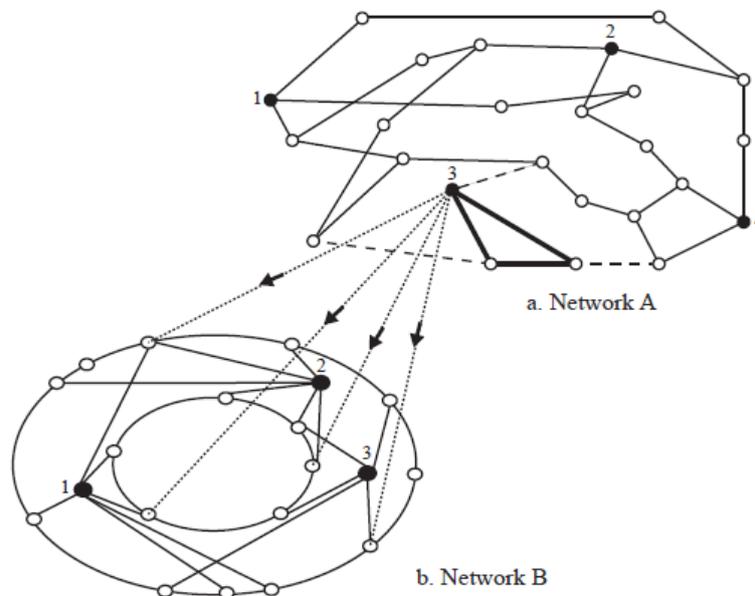


Figure 1. Two networks

This network was investigated in [4], Section 2.3. We assume that A is *DOWN* when all 4 its terminals (shown bold) become isolated from each other because of edge failures. Below is the edge cumulative spectrum calculated in [4: 68]:

$F(1) = \dots = F(7) = 0, F(8) = 0.00001, F(9) = 0.00016, F(10) = 0.00124,$
 $F(11) = 0.00612, F(12) = 0.02033, F(13) = 0.05281, F(14) = 0.11094,$
 $F(15) = 0.19166, F(16) = 0.28924, F(17) = 0.39887, F(18) = 0.50586,$
 $F(19) = 0.60720, F(20) = 0.69737, F(21) = 0.77295, F(22) = 0.83484,$
 $F(23) = 0.88400, F(24) = 0.92141, F(25) = 0.94906, F(26) = 0.96829,$
 $F(27) = 0.98165, F(28) = 0.99042, F(29) = 0.99578, F(30) = 0.99826,$
 $F(31) = 0.99963, F(32) = F(33) = F(34) = 1.$

Assume that the edges fail in a random order according to a Poisson process with parameter $\lambda = 1$, i.e. the average interval between two successive edge failures equals 1. After A has failed, its terminals 1, 2, 3, and 4 are randomly "attacking" $M_1 = 5, M_2 = 4, M_3 = 4, M_4 = 2$ non terminal nodes of B , respectively. These nodes are chosen in a random and independent way, and the maximal number of nodes which can be destroyed equals $R = M_1 + M_2 + M_3 + M_4 = 15$.

Network B is shown on Figure 1b. It has 20 nodes and 34 edges; nodes 1,2,3 are terminals. These nodes are the "hubs" of the network, and isolation of any of them from two others is considered as B DOWN state. This network has been studied in [5]. Below is the node cumulative D-spectrum of B , see [5]:

$F(1) = \dots = F(4) = 0, F(5) = 0.000686, F(6) = 0.007581, F(7) = 0.033789,$
 $F(8) = 0.097702, F(9) = 0.212468, F(10) = 0.375406, F(11) = 0.562010,$
 $F(12) = 0.739308, F(13) = 0.875172, F(14) = 0.957617, F(15) = 0.992610,$
 $F(16) = F(17) = 1.$

After A fails, the number of damaged nodes Y in B lies in the interval $[1, 15]$, and the probability that $Y = k$ nodes are damaged equals by (2)

$$p_k(15;17) = \binom{17}{k} \sum_{t=0}^k \binom{k}{t} (-1)^t \left(\frac{k-t}{17}\right)^{15} \tag{8}$$

98% of all probability of Y is concentrated in the interval $8 \leq Y \leq 13$, as one can see from the data below:

$$p_8 = 0.074, p_9 = 0.207, p_{10} = 0.312, p_{11} = 0.255, p_{12} = 0.110, p_{13} = 0.024.$$

Table 1 presents the values of $P(DOWN_B; t)$ for various t values. It is seen that the maximal failure probability of B does not exceed 0.417 and it is reached at time $t = 50$ when all edges of A have already failed.

Somewhat surprising is the fact that $R = 15$ "attacks" on 17 non terminal nodes of B result in a relatively low failure probability. This happens because many nodes receive more than one "ball" and some nodes, therefore, remain undamaged.

Let us investigate the dependence of $P(DOWN_B; 50)$ on R for $R > 15$. The corresponding data are presented in Table 2.

Table 1. $P(DOWN_B; t)$ as a function of t for $R = 15$

t	10	15	20	25	30	40	50
$P(DOWN_B; t)$.016	.112	.156	.358	.401	.416	.417

Table 2. $P(DOWN_B; 50)$ as a function of R

R	12	15	18	21	24	27	30	35
$P(DOWN_B; 50)$.214	.417	.602	.742	.837	.900	.940	.970

It is seen from this table that $P(DOWN_B;50)$ grows relatively slow with the increase of R . To guarantee that B fails with probability at least 0.90, 27 or more "attacks" need to be carried out from A on nodes of B . When, on the contrary, $R = 12$, the failure probability drops to 0.214. We conclude that B in our example is quite reliable and its reliability is rather sensitive to the total number of random "attacks" on the non terminal nodes of B .

It is expected that the "attacks" of A terminals will be more efficient if R is divided into several portions and each portion will be "attacking" a subset S_i of nodes, chosen in such a way that these subsets are not intersecting and $\bigcup_i S_i = V_B \setminus T_B$. As calculations show, separation into two subsets will provide a rather small increase of failure probability. For example, if $R = 20$ is divided into two equal portions "attacking" subsets of 9 and 8 nodes, then $P(DOWN_S;50) = 0.73$ while in the original setting this probability is equal 0.70.

5. Concluding Remarks

Our further research will be aimed at the extension of the above described model to the situation of *interconnected* networks, i.e. to the study of failure development in the presence of mutual dependence of networks A and B states. In the case of interconnection, it is interesting to investigate how the failures of both networks evolve in time and how are distributed the time instants of their failure.

References

1. David, F. N. & Barton, D. E. (1962). *Combinatorial Chance*. London: Charles Griffin & Co, Ltd.
2. Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291), 1025–1028. DOI 10.1038/nature08932.
3. Gertsbakh, Ilya & Shpungin, Yoseph. (2009). *Models of Network Reliability: Analysis, Combinatorics and Monte Carlo*. CRC Press.
4. Gertsbakh, Ilya & Shpungin, Yoseph. (2011). *Network Reliability and Resilience*. Heidelberg-Dordrecht-London-New York: Springer Verlag.
5. Gertsbakh, Ilya & Shpungin, Yoseph. (2011). Stochastic models of network survivability. *Quality Technology and Quantitative Management*, 9, 45–58.
6. Gertsbakh, Ilya & Shpungin, Yoseph. (2011). Probabilistic description of network behavior under random attack on its nodes. In Proceedings of the 4th Intern. Conf. on Risk Analysis, ICRA-4, 2011 (105–112). Nicosia: University of Cyprus.
7. Gutfrant, Alexander. (2011). Optimizing network topology for cascade resilience. Invited chapter. In *Handbook of Optimization in Complex Networks*. New York: Springer Verlag.
8. Samaniego, F. J. (2007). *System Signatures and Their Applications in Engineering Reliability*. Berlin, New York: Springer Verlag.