BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **16**, No 6
Special issue with selection of extended papers from 6th International Conference on Logistic, Informatics and Service Science LISS'2016

Sofia • 2016 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2016-0086

Structural Robustness of Unidirectional Dependent Networks Based on Attack Strategies

Longbang Ma[1]*, Ping Guo*[2]*, Juan Zhao*[2]*, Lei Qi*[1]

[1]*Simulation Training Center, Logistical Engineering University, Chongqing 401311, China*
[2]*Training Department, Logistical Engineering University, Chongqing 401311, China*
Emails: malongbang@163.com guopingleu@126.com zhaojuan82@126.com qilei@126.com

Abstract**:** *Current works have been focused on the robustness of single network and interdependent networks. However, to be more correct, the dependence of many real systems should be described as unidirectional. To study the structural robustness of networks with unidirectional dependence, the dependent networks named UDN are proposed, the description of the propagation of failures in them is given, as well as the introduction of the attack strategies that the probability of a node being attacked depends on the degree* (*DP attack*) *or on the betweenness* (*BP attack*) *of this node. The simulated results show that UDN is more vulnerable to BP attack when is first attacked a node with high betweenness. Compared with the Interacting Networks* (*IN*)*, the UDN is more fragile under the two attack's strategies.*

Keywords**:** *Structural robustness, two-layer networks, cascading failure.*

1. Introduction

In recent years, extensive efforts are put into studies to learn and understand the robustness of complex networks. Previous researches have mainly focused on the robustness of single, isolated networks which do not interact with or depend on other networks [1-4]. One important finding is the robustness of scale-free networks that include the Internet, social networks and cells [5]. It is well observed that such networks are robust under random removal but fragile under intentional attack. The effect of attack strategies on network robustness has been studied in many researches [2-6].

Recently, the robustness of two interdependent coupled networks has been studied [7-17]. Regards interdependent networks, most studies are restricted by the assumption that the number of nodes in the two networks or layers is the same and one-on-one mapping, so that every node in one network or layer has a corresponding node in the other system or layer. The failures of nodes in the one network will cause failures of corresponding nodes in the other network, and vice versa. The propagation of failures advances recursively. However, this assumption may not stand valid in the reality. For example, the failure of a train on a high-speed rail has no effect on its power supply network, but the failure of a power station in power supply network do result in the failure of high-speed rail. The function of unidirectional dependence also exists in different layers of IP network and the transportation network. In general, the foundational network or layer provides necessary conditions for the regular operation of service network or layer. Only when the corresponding node in foundational network or layer remains functional, the node in service network or layer can keep functioning. But the failure of a node in service network or layer apparently does not affect its supporting node in the foundational network or layer owing to the unidirectional dependence.

A type of dependent networks named UDN is proposed; their structural robustness is investigated with two attack strategies based on node connectivity named DP attack (depends on the degree) and BP attack (depends on the betweenness) in simulated situations. The study has filled in the blank of robustness research between the single network and interdependent network, and extends previous works with attack strategy, which can certainly help to further understand coupled network systems with unidirectional dependence.

The paper is structured as follows. The network model is proposed in Section 2. The propagation of failures in UDN is introduced in Section 3. In Section 4, the attack strategies are described. The results are analyzed in Section 5 and the conclusion is given in Section 6.

2. The model

To study the structural robustness, the Unidirectional Dependent Networks (UDN) are modeled. The UDN model is composed of two-layer networks which nodes are dependent unidirectionally. In the UDN model, the top layer is defined as the logical layer and the bottom one is called physical layer. The physical layer supports the logical layer in action, just like the physical layer supports the normal operation of the application layer in IP networks. It is assumed that each node of logical layer must be dependent on a node in the physical layer. For instance, if node 1 of logical layer stops functioning owing to the attack, node 1 of physical layer will not be affected. On the contrary, if node 1 of physical layer stops functioning then node 1 of logical layer stops functioning due to the dependence (Fig. 1). The number of nodes in logical layer is N^l, and N^p is the number of nodes in physical layer. N^l is less than N^p. Within each layer, the nodes are connected by connectivity links. Between the two layers, the nodes are connected by dependency links. β is used as the dependent parameter to describe the extent to which the logical layer depends on the physical layer, where $\beta= N^l/N^p$.

The Interacting Networks (IN) [18] is applied to make contrast with UDN. The IN is also composed of two or more networks which nodes are not dependent, this is indicated with only connectivity links and no dependency links existing between the two layers. The IN is frequently mentioned in the study of protein interaction networks.

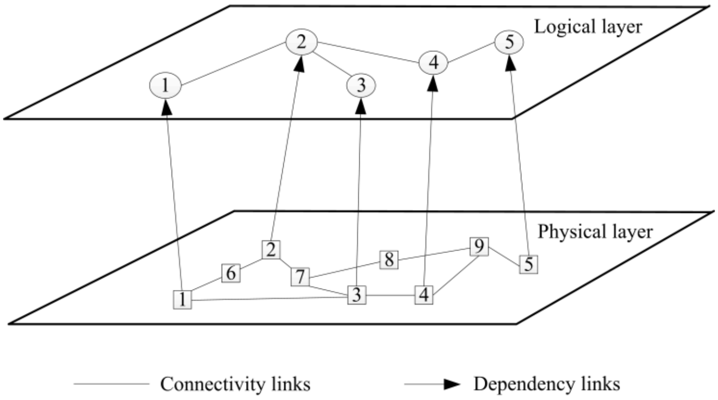


Fig. 1. An illustration of the UDN model with the logical layer and the physical layer

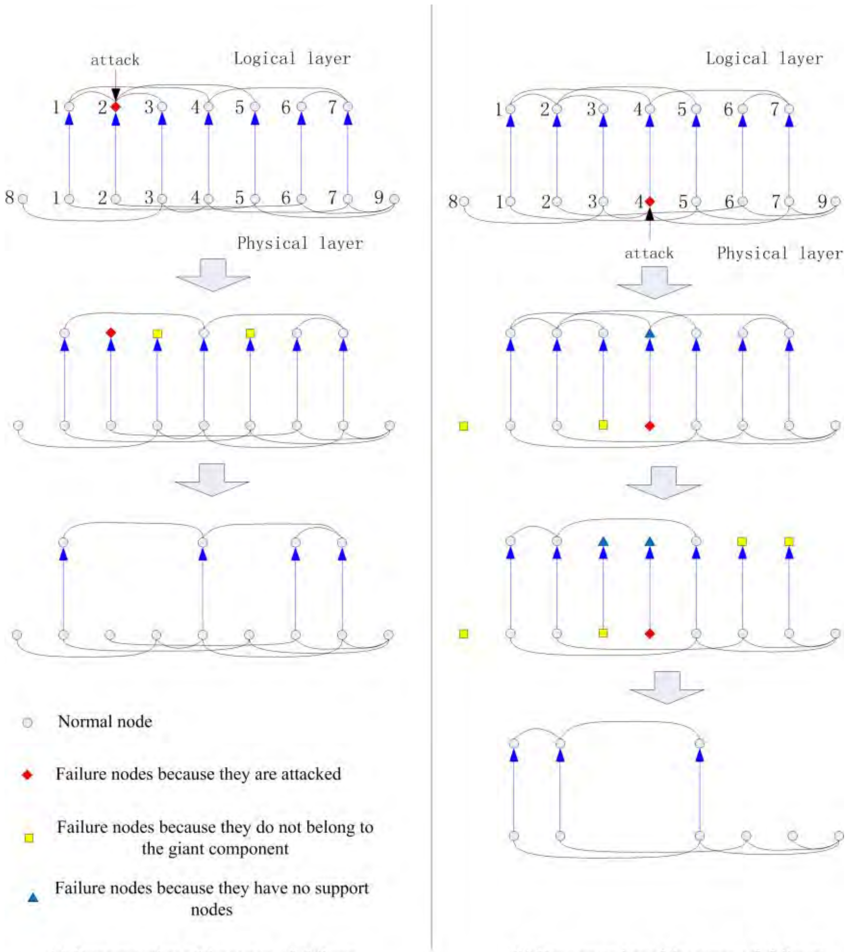
3. The propagation of failures in UDN

In general, it is assumed that only nodes that belong to a giant connected component of each network remain functional. Besides, to be functional, a node in the logical layer must have one functional support node in the physical layer. This assumption leads to different cascading failures in each layer.

In this paper, the structural failure is defined to describe the node failure owing to no connection to the giant component. Similarly, if the absence of support node causes the failure of the node, this is called functional failure. Thus the failures of nodes in UDN can be divided into three types (Fig. 2): Attacked failed nodes, structurally failed nodes and functionally failed nodes. The IN only has attacked failure and structural failure without the functional failure in the propagation of failures.

The propagation of failures is demonstrated on Fig. 2, where the case of attacking a node in the logical layer is presented on Fig. 2a and one node in the physical layer on Fig. 2b. The state remains stable when the cascading failures end. At every step of propagation of failures, the network experiences further failures and the number of fault nodes increases. The propagation of failures of one attacked node is shown in logical layer (Fig. 2a). Initially, the node of logical layer L_2 is attacked, followed by the failures of L_3 and L_5 due to the structural failure. The failed nodes and failed links are removed. After the cascade of failures, four nodes are functional in logical layer and the nodes in physical layer are not affected.

Different from the propagation of failures of one attacked node in the logical layer, the propagation of failures of one attacked node in physical layer is complicated (Fig. 2b). At first, the node of physical layer P_4 is attacked and failed, leading to the structural failures at P_3 and P_8. Then, L_3 and L_4 suffer functional failure because of the absence of dependent nodes, P_3 and P_4. Finally, L_4 leads to structural failure of nodes L_6 and L_7, so that the UDN only has three functioning nodes in logical layer and six functioning nodes in the physical layer. After the propagation of failures, all nodes in both giant components are connected and each node of the logical layer is supported by the corresponding node on the physical layer.


attack
Logical layer
1 2 3 4 5 6 7
8 1 2 3 4 5 6 7 9
Physical layer
Logical layer
1 2 3 4 5 6 7
8 1 2 3 4 5 6 7 9
attack
Physical layer
○ Normal node
◆ Failure nodes because they are attacked
□ Failure nodes because they do not belong to the giant component
▲ Failure nodes because they have no support nodes

(a) Demonstration of the stages of failures because the node is attacked in logical layer

(b) Demonstration of the stages of failures because the node is attacked in physical layer

Fig. 2. The propagation of failures in UDN

4. Attack strategy

Attack strategy focuses the selection process of the order in which nodes are attacked. In the previous researches, the random removal and the targeted intentional attack are the most commonly used strategies. The random removal generates the attacked order based on random probability. The targeted intentional attack uses the node connectivity to generate the descending attack sequence.

However, the targeted intentional attack requires the input of all learning of network topology after every attack which is time-consuming and complex in computing. Besides, it is too ideal that the node with the most connectivity is always first attacked.

An easier and more realistic operation is to use the initial knowledge of network structure to select the nodes in the attack order and remove nodes one by one starting from the node with the probability of being attacked based on its connectivity. Degree and betweenness are used to characterize the connectivity of the network in this paper. When nodes are attacked by different connectivity parameters, two attack strategies will occur.

4.1. Attack strategy based on node degree

This attack strategy uses the node degree to decide the probability $W(i)$ of node i being attacked and thus is defined as "DP attack" throughout the current paper. The $W(i)$ is defined for a node i as follows:

$$W(i) = \frac{D_i^{\alpha}}{\sum_{i=1}^{N} D_i^{\alpha}}, \tag{1}$$

where D_i is the node degree of i, and N is the number of nodes. Attack parameters α, $+\infty<\alpha<-\infty$, can adjust the probability. In the situation $\alpha > 0$, nodes with a larger degree are more vulnerable, whereas for $\alpha < 0$, nodes with a larger degree are less vulnerable. $\alpha = 0$ represents the known random removal, and $\alpha \to +\infty$ represents the targeted intentional attack. This attack strategy can only use the partial knowledge of the network, just as the degree, which means that the number of neighbours without who are the neighbours can decide the probability of a node being attacked.

4.2. Attack strategy based on the vertex betweenness

This attack strategy is called "BP attack" use the vertex betweenness to calculate the probability $V(i)$ of node i being attacked.

The generalized betweenness B_i of node i is defined as in [19]:

$$B_i = \sum_{j \neq k \neq i} \frac{l_{jk}(i)}{l_{jk}}, \tag{2}$$

where l_{jk} is the number of all the shortest paths from node j to node k; $l_{jk}(i)$ is the number of all the shortest paths from node j to node k that pass node i.

The $V(i)$ is defined as

$$V(i) = \frac{B_i^{\alpha}}{\sum_{i=1}^{N} B_i^{\alpha}}, \tag{3}$$

where α plays the same role as it in the $W(i)$. However, BP attack requires the knowledge of the whole network structure to calculate $V(i)$, which is more complex and trivial than $W(i)$.

Either DP attack or BP attack is used to obtain the attack order. The node is removed by the order in every attack step. p is defined as the ratio of attacked nodes to the original network nodes in every attack step. The size S is defined as the fraction of nodes contained in the giant component in every attack step, describing the characterization of the robustness of the network. The integrity of a network is destroyed when the S=0 after a critical percentage p_c of the networks nodes have been attacked. p_c is the critical threshold for a given network with certain attack strategies, which can represent the robustness of the network under different attack strategies.

The procedures of the structural robustness of UDN can be illustrated as follows.

Step 1. According to the selected attack strategy, use the initial knowledge of UDN structure to calculate

$$[W(1), W(2), W(3),\ldots, W(N)] \text{ or } [V(1), V(2), V(3),\ldots, V(N)].$$

Step 2. Calculate the attack order sequence $[i, j, k,\ldots, m]$ on the basis of (i).

Step 3. Follow the number in the sequence to attack each node in UDN. If the current node is failed due to a propagation of failures, then select the next node to attack in the sequence. Calculate p and S at every attack step. Record p_c when S=0.

5. Simulation results

In this section, simulation results are shown for DP attack and BP attack in UDN compared with IN. The purpose of the simulation is to demonstrate the impact on robustness of a given UDN under DP attack and BP attack. Moreover, the function of a unidirectional dependence is also explained by comparing the robustness with UDN and IN. We assume a UDN with N^l =108 and N^p =127 which is abstracted from the IP network. The IN has the same structure as the UDN where the dependency links in UDN is changed to the connectivity links in IN.

To understand the difference between the probabilities of getting vulnerable in DP attack and BP attack, $W(i)$ and $V(i)$ are calculated when $\alpha = 1$ since the degree and betweenness are initial values in this case. Fig. 3 shows the probability distribution of each node attacked under DP attack and BP attack. $W(i)$ and $V(i)$ are sorted in descending order. The values of $W(i)$ and $V(i)$ drop rapidly for i<33 while they are tended towards stable for $i > 33$.As shown in this figure, the distribution of $V(i)$ is more concentrated than $W(i)$, which indicates that the node with high betweenness is more vulnerable. When $i > 33$, the values of $W(i)$ is always greater than the values of $V(i)$, indicating that a lot of low degree nodes are more vulnerable in this case.

In order to show the propagation of failures in UDN, the UDN is attacked with two strategies as $\alpha = 2$ and likewise, the IN is also attacked in the same way. Each result is the average of the results after 40 times of simulation. By changing the ratio of attacked nodes p and counting S, it could be obtained the approximate value for critical percentage p_c at UDN and IN under different attack strategies. Fig. 4 shows the relative size of largest component S of the superposed network under the attack strategies with the removal of nodes of fraction p. As shown in this figure, S

obviously decreases with p and reduces to zero at a certain value of p_c. When 3% nodes are attacked, S is remarkably less than 1%. Either in UDN or IN, the S is decreasing more rapidly with BP attack than with DP attack. The differences among the removal procedures are not significant when $p > 0.3$. However, as the attack proceeds, the critical percentage p_c is detected in the order with $p_c^{bu} < p_c^{du} < p_c^{bi} < p_c^{di}$, implying that the BP attack is more harmful than DP attack in UDN and IN in the case of $\alpha = 2$.

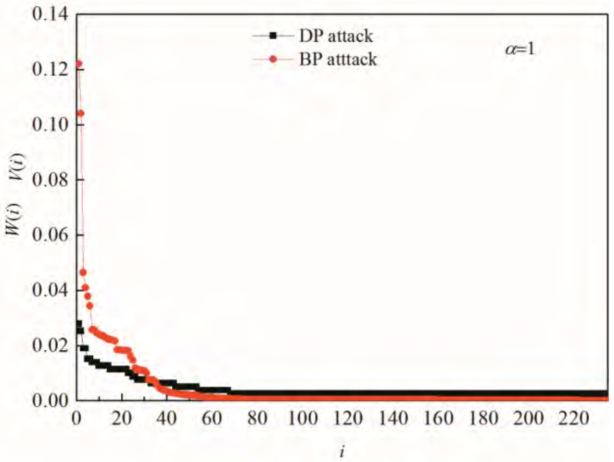


Fig. 3. The probability distribution of each node attacked under different attack strategies

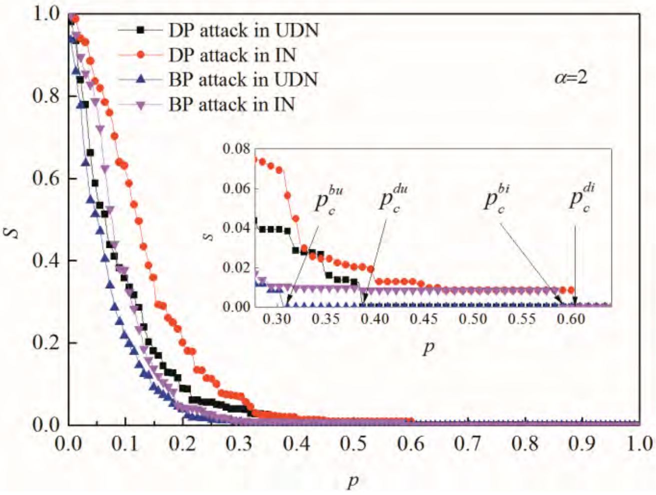


Fig. 4. The network fragmentation under attack in UDN and IN

To study the effect of the different probabilities of being attacked under different attack strategies in UDN, the simulation results are organized to explain the relationship between p_c and α in the UDN. As shown on Fig. 5, it is remarkable that for every attack strategy in UDN, p_c declines with increasing α overall by descending slowly for negative α and decreasing rapidly for very small positive α. p_c for BP attack is higher than that for DP attack, usually between 0.8 and 0.6 with negative α, revealing that the DP attack is more harmful while the node with low connectivity is firstly attacked and the attack strategy is not efficient enough to destroy the UDN. On the contrary to previous results, when $\alpha > 0$, p_c for DP attack is higher than that for BP attack and reduces gradually to 0.25. Accordingly, UDN is more vulnerable by attacking node firstly with high betweenness, where the attack strategy is efficient. When $\alpha = 0$, all the strategies become the random attack, so the results are the same.

To analyze the effect of the unidirectional dependence in UDN, the comparison is made between the simulation results of UDN and that of IN, shown in Fig. 5. As a whole, the p_c in UDN is less than that in IN, which clearly confirms that the UDN is more vulnerable to the attack than the IN, resulting from the fact that the unidirectional dependence has reduced the robustness of UDN. In other words, compared to the IN, the reduction of the robustness of the UDN is due to the fact that attacking the nodes of physical layer can cause cascading failure not only in the physical layer but also in the logical layer.

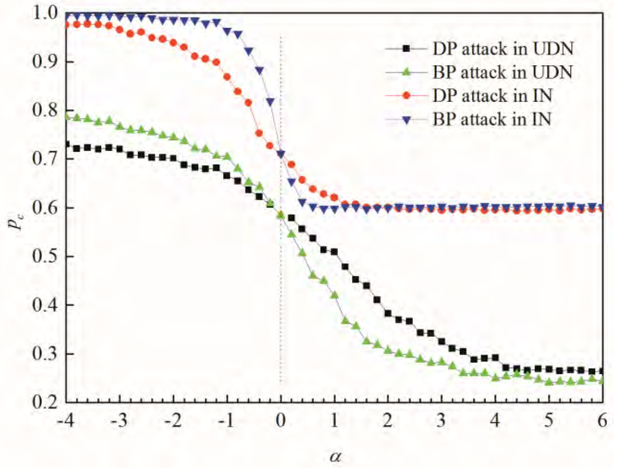


Fig. 5. The values of p_c vs α with UDN and IN under different attack strategies

In order to spot the effect of dependent parameter in UDN's robustness, 9 values with different dependencies are chosen, as shown on Fig. 6. With each value that corresponds to the physical layer of the network remaining unchanged, the logical network layer is reduced according to the descending order based on node numbers. The initial logical layer has 127 nodes with β=0.85. When β=0, the logical layer of the network does not exist, with only the physical layer left in the network. It can be seen from Fig. 6 that when α is less than 1.1, p_c decreases with increasing α. The larger the value of β is, the greater the corresponding values of p_c will be, which indicates that the high dependence of UDN network has strong survivability in the DP attack strategy since larger degree nodes are less vulnerable. α being greater than or equal 1.1 and β being 0.25, 0.35 and 0.85, p_c gradually decreases. In the rest of the case, p_c declines more obviously, owing to the logical layer network structure with different β, indicating that when the nodes with larger degree are more vulnerable, the UDN survivability is less relevant to the dependency, but more relevant to the logical layer network structure.

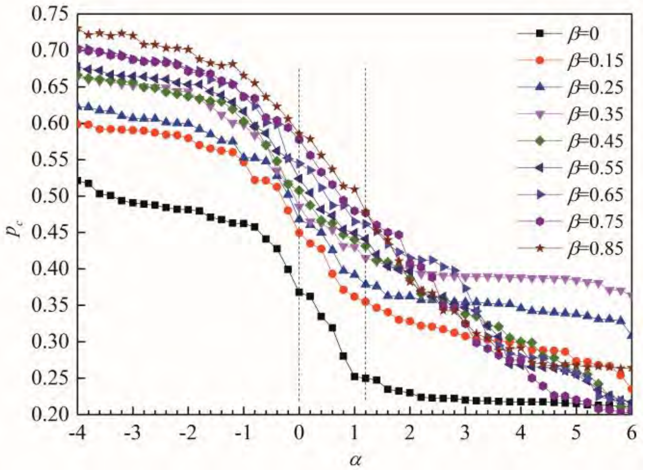


Fig. 6. The values of p_c vs β with UDN under DP attack strategy

6. Conclusions

In this paper, a dependent network named UDN is proposed, which structural robustness is investigated in two attack strategies based on node connectivity named DP attack and BP attack. The UDN is vulnerable to attack strategy in which the node with high connectivity is firstly attacked, especially in BP attack. The robustness of UDN is strong when its node is firstly attacked with less connectivity. The unidirectional dependence between the two layers reduces the robustness of UDN. The high dependence of UDN network has strong survivability in the DP attack strategy where the nodes with larger degree are less vulnerable. When the nodes with larger degree are more vulnerable, the UDN survivability is less relevant to the dependence, but more relevant to the logical layer network structure.

References

1. Callaway, D. S., M. E. J. Newman, S. H. Strogatz et al. Network Robustness and Fragility: Percolation on Random Graphs. – Physical Review Letters, Vol. **85**, 2000, No 25, pp. 5468-5471.
2. Gallos, L. K., R. Cohen, P. Argyrakis et al. Stability and Topology of Scale-Free Networks under Attack and Defense Strategies. – Physical Review Letters, Vol. **94**, 2005, No 18, pp. 188701.
3. Moreno, Y., J. Gómez, A. Pacheco. Instability of Scale-Free Networks under Node-Breaking Avalanches. – Europhysics Letters, Vol. **58**, 2002, No 4, p. 630.
4. Pocock, M. J., D. M. Evans, J. Memmott. The Robustness and Restoration of a Network of Ecological Networks. – Science, Vol. **335**, 2012, No 6071, pp. 973-977.

5. Albert, R., H. Jeong, A.-L. Barabási. Error and Attack Tolerance of Complex Networks. – Nature, Vol. **406**, 2000, No 6794, pp. 378-382.
6. Holme, P., B. J. Kim, C. N. Yoon et al. Attack Vulnerability of Complex Networks. – Physical Review E, Vol. **65**, 2002, No 5.
7. Shekhtman, L. M., Y. Berezin, M. M. Danziger et al. Robustness of a Network Formed of Spatially Embedded Networks. – Physical Review E, Vol. **90**, 2014, No 1.
8. Schneider, C. M., N. Yazdani, N. A. Araujo et al. Towards Designing Robust Coupled Networks. – Scientific Reports, Vol. **3**, 2013.
9. Morris, R. G., M. Barthelemy. Interdependent Networks: The Fragility of Control. – Scientific Reports, Vol. **3**, 2013.
10. Parshani, R., S. V. Buldyrev, S. Havlin. Interdependent Networks: Reducing the Coupling Strength Leads to a Change from a First to Second Order Percolation Transition. – Physical Review Letters, Vol. **105**, 2010, No 4.
11. Buldyrev, S. V., N. W. Shere, G. A. Cwilich. Interdependent Networks with Identical Degrees of Mutually Dependent Nodes. – Physical Review E, Vol. **83**, 2011, No 1.
12. Boccaletti, S., G. Bianconi, R. Criado et al. The Structure and Dynamics of Multilayer Networks. – Physics Reports, Vol. **544**, 2014, No 1, pp. 1-122.
13. Shao, J., S. V. Buldyrev, S. Havlin et al. Cascade of Failures in Coupled Network Systems with Multiple Support-Dependence Relations. – Physical Review E, Vol. **83**, 2011, No 3.
14. Shao, S., X. Huang, H. E. Stanley et al. Robustness of a Partially Interdependent Network Formed of Clustered Networks. – Physical Review E, Vol. **89**, 2014, No 3.
15. Shimada, T. A Universal Transition in the Robustness of Evolving Open Systems. – Scientific Reports, Vol. **4**, 2014.
16. Su, Z., L. Li, H. Peng et al. Robustness of Interrelated Traffic Networks to Cascading Failures. – Scientific Reports, Vol. **4**, 2014.
17. Gao, J., S. V. Buldyrev, S. Havlin et al. Robustness of a Network of Networks. – Physical Review Letters, Vol. **107**, 2011, No 19, pp. 195701-1-195701-5.
18. Dong, G., R. Du, L. Tian et al. Percolation on Interacting Networks with Feedback-Dependency Links. – Chaos: An Interdisciplinary Journal of Nonlinear Science, Vol. **25**, 2015, No 1.
19. Newman, M. E. Scientific Collaboration Networks. II. Shortest Paths, Weighted Networks, and Centrality. – Physical Review E, Vol. **64**, 2001, No 1.