Analysis of Cascading Failure Based on a New Load Redistribution Model

Tao Wang *
A School of Mathematics and Physics,
North China Electric Power University,
Baoding, Hebei, 071003, China
wtwxx@126.com
* Corresponding Author

Hongjue Wang
A School of Mathematics and Physics,
North China Electric Power University,
Baoding, Hebei, 071003, China
wangybwd@163.com

Yunzhu Li
A School of Mathematics and Physics,
North China Electric Power University,
Baoding, Hebei, 071003, China
benz1250@163.com

Abstract—Cascading failure has drawn increasing attention to security problems due to the failure of a part triggers the failure of successive parts and even the entire network. In order to avoid cascading propagation more effectively, based on the local preferential redistribution rule of the failed node's load, researchers propose a new allocate strategy, considering the product of the degree and remaining capacity of the node's neighboring nodes. Here, researchers investigate the effect of the new allocate strategy for the robustness against cascading failures on a typical network, i.e. BA scale-free networks. Compared with two previous allocate methods, researchers find that our presented model is more robust than the previous models by the simulation and analysis in BA scale-free network. Moreover, researchers investigate how S_{attack} changes depending on some of the parameters in our model. It is also found that the network robustness has a positive correlation with the value of α in the ranges of the larger avalanche, whereas, on the contrary, the smaller the value of α is the more robust the network is. Researchers can apply the result of the correlation between the parameters and the network robustness to allocate loads in real network.

Keywords- Complex Networks; Preferential Probability; Load Redistribution; Robustness; Cascading Failure

I. INTRODUCTION

Many complex systems can be described as complex networks, from biological or ecological networks [1] in nature to communications [2], power transmission [3] and social [4] networks in social life, which are characterized by large scale, complicated structure and spatiotemporal evolution process [5]. However, successive failure phenomenon is widely existed in many actual complex networks. Both the major power blackout in 2003 and the south snow disaster in 2008 not only led to the collapse of electric power system, but also affected many other infrastructures, including the closure of the financial institutions and uncontrolled transportation system. The similar phenomenon among these networks is called cascading failure, the failure of a part triggers the failure of successive parts through the coupling relationship between nodes, which has strong destructive power and influence.

In recent years, network cascading failures and robustness have been widely investigated [6,7] by domestic and foreign researchers. Network robustness can be defined as the ability of a system to resist change without adapting its initial stable configuration [8], and be divided into static robustness and dynamic robustness [9]. The difference between them is whether the fault node or edge can lead to other nodes or the edge of failure. It makes sense to only study dynamic robustness which refers to network structure and dynamic behavior in this article.

In related researches of the cascading failure, the key is to establish cascading model at first including how to distribution load and capacity to the nodes in the network and how to redistribute the load on the nodes in the case of the node was attacked. The research of the load-capacity model the most widely used is began in the Literature [10], which proposed the initial load of the each node is the same and capacity obey Weibull distribution, its load is just equally transferred to the non-failed nodes directly linked to it in the case of the node fails. It suffers from the shortcomings referring to the little practical significance. In order to overcome the problem, Motter and Lai [11] proposed the another load-capacity model, including the initial load of the node defined as betweenness and capacity is linearly proportional to the initial load, but it is not practical that the solve of the betweenness refer to the global information of the network, computational cost is larger, more difficult to solve. Thus, Wang et al [12] proposed the cascading failure model based on a load local redistribution rule and investigated cascading failures on the typical network. Researchers only need to know the local information of each node by studying the relation between the initial load and the node degrees. Though it can make the problem easier, it is no considering that the remaining capacity of its neighbor nodes. Junliang Ren [13,14] presented a new strategy of load redistribution based on the remaining capacity of the neighboring nodes, and it can reduce the size of cascading failures about 10%

compared with based on the degree of the neighboring node. The model can avoid the access of the network global information and it also take into account the effect of residual capacity on the cascading propagation.

In this paper, researchers consider such case that the one neighbor node has the biggest remaining capacity, but its degree is one, means it is a leaf node compared with the other nodes which has not the biggest remaining capacity, but the number of the nodes directly linked to it is exceed one. Researchers can allocate the more load to the latter but not the former node. So researchers propose a novel redistribution strategy, considering both remaining capacity and the degree of the neighbor nodes, to improve the network robustness against the cascading failures.

In the following sections, researchers will discuss this model in detail. Sec. 2 develops the cascading model in three aspects including the definition of the load and capacity and a novel redistribution strategy. Experimental analysis and results are illustrated in Sec. 3. Finally, conclusion is made in Sec. 4.

II. THR MODEL

In the normal initial state, one or several of the nodes that form the network is subjected to a small initial disturbance, which is sufficient to collapse the entire network simply owning to the dynamics of the load redistribution. In other words, since the removal of the failed node changes the balance of the load distribution of the network and leads to a global redistribution of loads among the rest of nodes [10,15], its load is transferred to the non-failed nodes directly linked to it according to the redistribution strategy, but if the capacity of these nodes cannot yet handle the load, this may provoke one or several of the neighbor nodes to breakdown and remove simultaneously from the network, by repeatedly applying the rules stated above, a cascading process could start that lasts until the system arrives at a new equilibrium state where all the nodes support a load lower than their capacity.

Taking the above process into account, researchers briefly introduce the cascading model proposed by Wang and Rong [16].

At first, researchers assume that the load of the node i has a certain correlation with its degree, and the load on node i is then

$$L_i(0) = k_i^{\alpha}, i = 1, 2, \ldots, N \tag{1}$$

Where N is the initial number of nodes in the network and k_i being the degree of node i, where the constant α is a positive tunable parameter, governing the strength and distribution of the node initial load, it is obvious that the bigger the value of α is the more heterogeneous distribution is, and the stronger initial load of the node is.

Secondly, owing to the capacity of the node is the maximum load that the node can handle and limited by the cost on the real-life network in general, researchers simply assume the capacity C_i of node i to handle the load to be proportional to its initial load $L_i(0)$ by a proportionality factor β, i.e.,

$$C_i = (1+\beta)L_i(0) \tag{2}$$

Where tolerant parameter $\beta \geq 0$. The node operates in a free-flow regime if $L_i \leq C_i$; otherwise the node is assumed to fail and is removed from the network. The condition $\beta \geq 0$ means that no node is overloaded and the entire network is normal operation in the initial state, i.e. $L_i(0) \leq C_i$.

Inspired by the two previous methods in Refs [13, 16], therefore, researchers will also adopt the preferential redistribution mechanism and propose a new load redistribution strategy, the main difference with respect to previous allocate strategies is that the more additional load preferentially redistribute along the edge connected with not just the bigger remaining capacity but also the bigger degree among the neighbor nodes of the removed node, namely, the additional load of the failed node will be redistributed to its neighbor nodes according to preferential probability Π_j, i.e.

$$\Pi_j = \frac{k_j^{\alpha}(\Delta C_j)^{\gamma}}{\sum_{m\in\Gamma_i} k_m^{\alpha}(\Delta C_m)^{\gamma}} \tag{3}$$

Where, Γ_i is the set of the neighbor nodes of the removed node i.

According to the proportion of the product of remaining capacity and degree among its neighbor nodes, the additional load ΔL_{ji} received by node j, which is a neighbor node of the failed node i, is

$$\Delta L_{ji} = L_i \frac{k_j^{\alpha}(\Delta C_j)^{\gamma}}{\sum_{m\in\Gamma_i} k_m^{\alpha}(\Delta C_m)^{\gamma}} \tag{4}$$

Since each node has a limited capacity to handle the load, so for the node j, if $L_j + \Delta L_{ij} > C_j$, then node j will be broken and induce further redistribution of flow $L_j + \Delta L_{ij}$ and potentially further other nodes breaking.

Fig. 1 shows the load redistribution triggered by node removal, where node i is removed, and the load of the node i is redistributed to its neighboring nodes i.e., nodes j_1, j_2, j_3, j_4 and j_5 ,according to their preferential probabilities. Among these neighboring nodes, the one with the bigger the product of the degree and the remaining capacity will receive higher shared load from the removed node. The weight of the solid arrows represent the degree of the additional load is allocated to its neighboring nodes from the removed node. For example, the degree of the neighboring nodes j_1, j_2, j_3, j_4, j_5 are 5, 4, 1, 3, 2, and the remaining capacity are 0.5, 2, 3, 1.5, 2, respectively. It is obvious that the node which possesses the maximum product of the degree and the remaining capacity is node j_2, and node j_4 possesses the minimum product, so node i allocate the more shared load to the node j_2, and the less shared load to the node j_4.

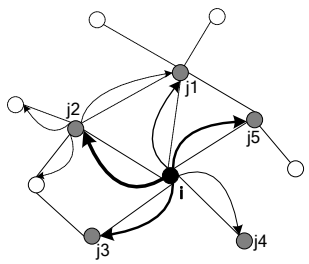


Figure 1. Illustration of cascading failure triggered by removing a single node

III. THE ANALYSIS OF CASCADING FAILURE MODEL

Owing to BA scale-free network is almost in accordance with real networks, researchers choose BA scale-free network as the research object to investigate the network robustness by large-scale numerical simulations analysis, here researchers will adopt the normalized avalanche size proposed by Wang and Rong [17] to quantify the robustness.

Assuming that the potential cascading failure is triggered by cutting a single node and cascading failures finish once no node's load exceeds its capacity.

Next, researchers briefly introduce a key measure of the average avalanche size, i.e.

$$S_{average} = \sum_{i \in N} s_i / n \tag{5}$$

Where s_i is defined as the number of broken nodes induced by removing node i, and N and n represents the set and the number of all nodes in the network, respectively. It is evident that $0 \le S_{average} \le \mathrm{n}-1$.

To make a meaningful comparison of the effect on the network robustness, researchers use the normalized avalanche size S_{attack} to quantify the network robustness, i.e.

$$S_{attack} = \sum_{i \in A} s_i / ((n-1)\mathrm{N}_A) \tag{6}$$

Where A and N_A representing the set and the number of the nodes attacked, respectively.

According to the role of parameter β in cascading failures, the network robustness is quantified by β_c for the certain the value of α and γ at which the network exhibits a "critical" behavior, i.e., a transition from a stationary state to collapse. Researchers will investigate the attack efficiency by the critical threshold β_c, It is evident that the smaller the value of β_c, the stronger network robustness against cascading failures.

Next, researchers will perform the large-scale numerical simulations of the cascading process produced by applying the new allocate strategy stated above and compare with the previous methods under the same network structure to see if the current model can achieve better performance compared with previous models. Researchers consider first the 1000-nodes and average degree <k>=4 BA scale-free network.

In Fig. 2, the red one shows allocate the load on the failed node by the new allocate strategy to the neighboring nodes under attack. In the case of $\alpha = 1.0$, when $\beta \ge 0.4$, $S_{attack} \approx 0$ means the largest component of the network remain 100% of the original one. While $\beta < 0.4$, the slope of the red one in the graph increase more significantly. The other two color lines represent previous allocate strategies respectively, there is a small difference between random allocate and average allocate in the all above cases. When $\beta \ge 0.8$ for the average allocate strategies, $S_{attack} \approx 0$, and when $\beta \ge 0.4$ for the random allocate strategies, $S_{attack} \approx 0$. It shows that the critical threshold β_c in the current model is smaller than the previous models. Moreover, if researchers allocate the load on the failed node according to the new redistribution strategy proposed in the case of $\alpha = 1.0$ and $\beta = 0.4$, more than 30% of the nodes are affected. For the 1000-node networks used in our simulations, it means that a cascade triggered by removing a single node leads to more than 300 others failure, while the current strategies can protect about 100% of network when attack appears under the same condition. The performance is much better than previous defenses.

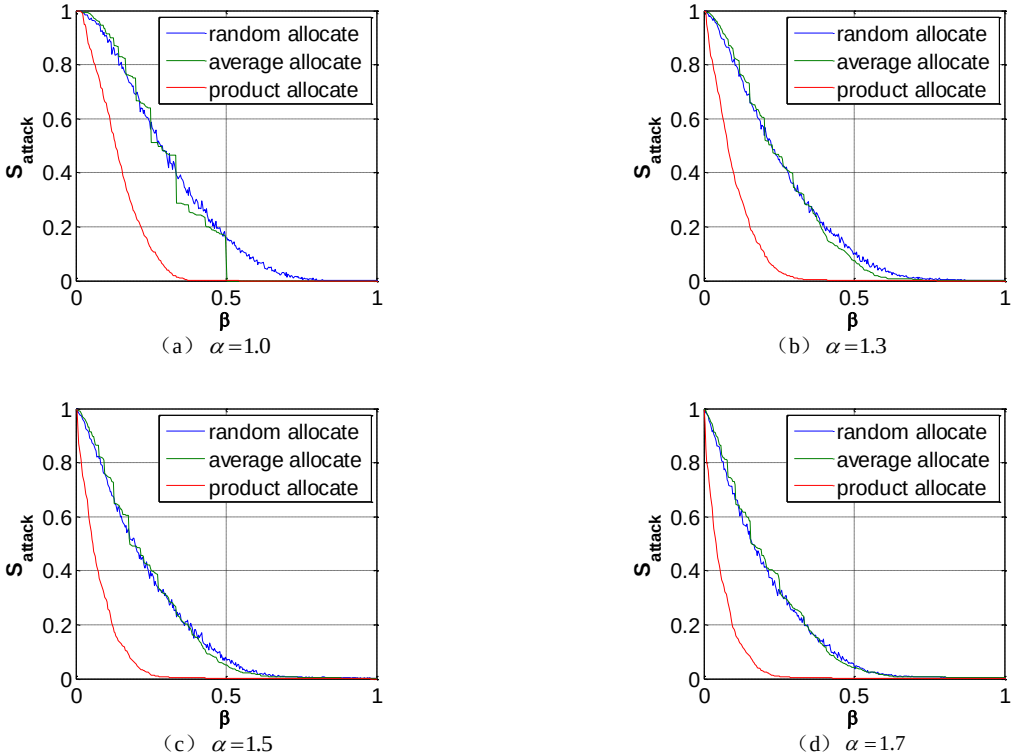
It is easy to find that these curves in the Fig. 2 have almost the same trend, no matter what kinds of allocation method, researchers can obtain that the index S_{attack} has a negative correlation with tolerance parameter β, i.e. the bigger the parameter β, the smaller the index S_{attack} and the more robust the network. But so as to improve the robustness by increasing the β will raise the cost. In what follows, according to our model, researchers further investigate the relation between the network robustness level and some parameters to effectively defense against cascading failures under the limited the cost.

Fig. 3 shows that the avalanche size S_{attack} as a function of the tolerance parameter β for the fixed γ and the various values of α. Researchers in detail compare the relation between index S_{attack} and tolerance parameter β at various value of α, in the ranges of the larger avalanche sizes, and find that these curves in the Fig. 3 have almost the same trend which index S_{attack} decrease as the value of β grows, while are remarkably different for different values α, for a fixed tolerance parameter β, the robustness has significantly positive correlation with the value of α, namely the bigger the value of α is, the bigger the S_{attack} is, and the more robust the network is.

Whereas in the ranges of the smaller avalanche sizes as was shown in the Fig. 4, there is the contrary result that the network robustness has a negative correlation with the value of α, i.e., the smaller the value of α is, the bigger the S_{attack} is, and the more robust the network is.

Moreover, the dependences of β_c on α are also studied as shown in the inset to Fig. 4 and it is found that the value of β_c shifts to a smaller value with increasing tunable parameter α. Researchers see that cascading failure is induced and enhanced when the tolerance parameter value is smaller than the threshold β_c, thus, these phenomena show that the larger α is the more robust the network is in BA scale-free networks. The

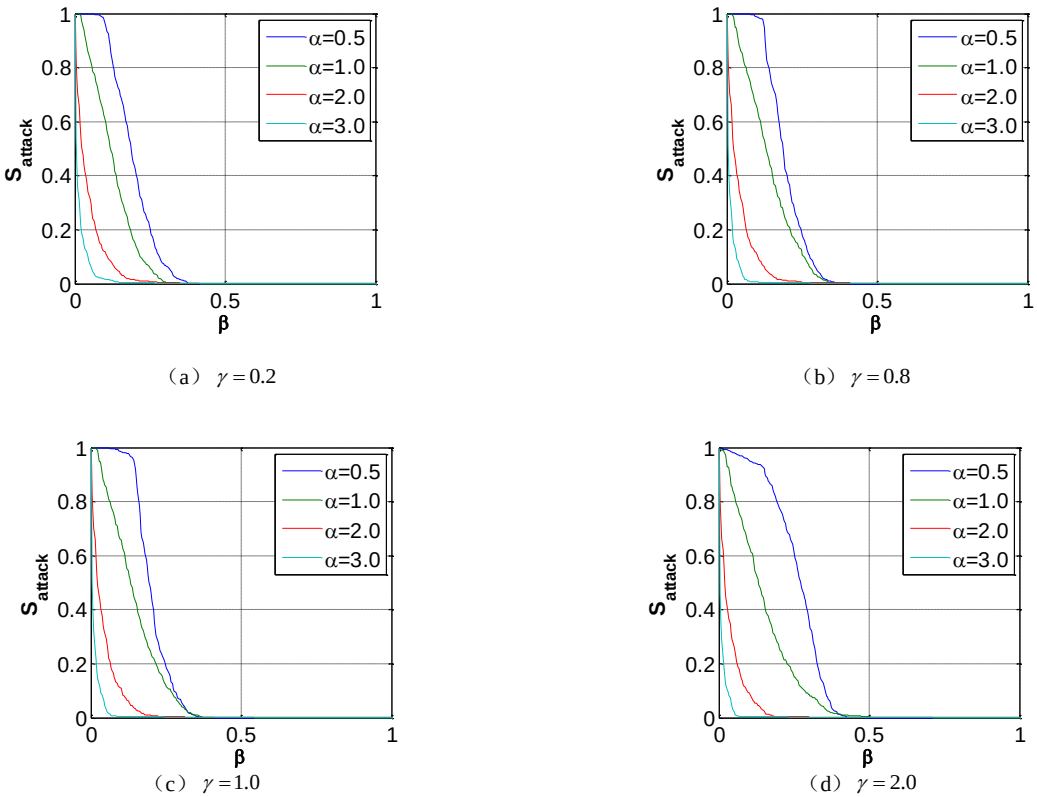
critical threshold β_c is a monotonously increasing function on parameter α .



（a） $\alpha=1.0$ （b） $\alpha=1.3$

（c） $\alpha=1.5$ （d） $\alpha=1.7$

Figure 2. Demonstration of effect of three kinds of the load redistribution strategies subject to node removal on BA.



（a） $\gamma=0.2$ （b） $\gamma=0.8$

（c） $\gamma=1.0$ （d） $\gamma=2.0$

Figure 3. Demonstration of the relation between the index Sattack in the ranges of the larger avalanche and tolerance parameter β on BA scale-free networks

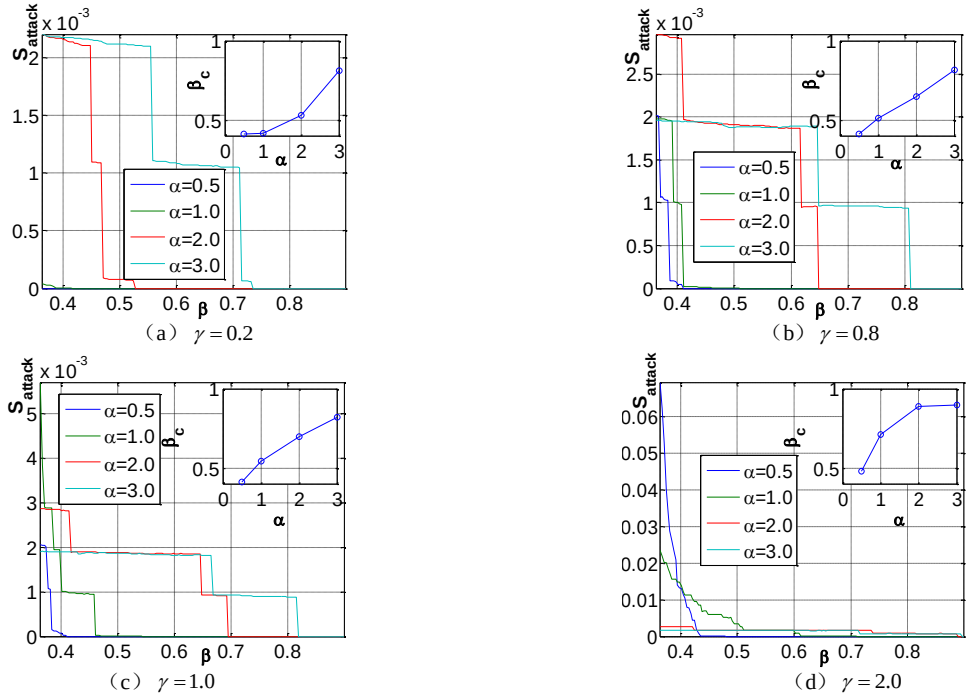


Figure 4. Demonstration of the relation between the index Sattack in the ranges of the smaller avalanche and tolerance parameter β on BA scale-free networks, where the insets show the dependences of βc on α.

IV. CONCLUSIONS

In this paper, researchers proposed the new allocate strategy which according to the proportion of the product of the remaining capacity and degree to improve the robustness of BA scale-free networks against the cascading failures while keeping the network topology structure constant. By large-scale numerical simulation analysis, it is conclude that researchers can get higher robustness of network than previous model with the same amount of resource. Researchers investigated how S_{attack} changes depending on some of the parameters in our model. It is also found that the lager α is the more robust the BA network is. Researchers can apply the result of the correlation between the parameters and the network robustness to allocate loads in real network.

ACKNOWLEDGMENT

This work is supported by the Fundamental Research Funds for the Central Universities (Grant No. 13MS108). The authors would like to express sincere appreciation to the anonymous referees for their detailed and helpful comments to improve the quality of the paper.

REFERENCES

[1] Han, Jing-Dong J, Nicolas Bertin, Tong Hao et al. Evidence for dynamically organized modularity in the yeast protein–protein interaction network [J]. Nature, 2004, 430(6995): 88-93.

[2] Broder A, Kumar R, Maghoul F, et al. Graph structure in the web [J]. Computer networks, 2000, 33(1): 309-320.

[3] Carreras B A, Lynch V E, Dobson I, et al. Critical points and transitions in an electric power transmission model for cascading failure blackouts [J]. Chaos: An interdisciplinary journal of nonlinear science, 2002, 12(4): 985-994.

[4] Brenner T. Implications of routine-based learning for decision making [J]. European Journal of Economic and Social Systems, 2001, 15(3): 131-152.

[5] Newman M E J. The structure and function of complex networks [J]. SIAM review, 2003, 45(2): 167-256.

[6] Cohen R, Erez K, Ben-Avraham D, et al. Breakdown of the Internet under intentional attack[J]. Physical review letters, 2001, 86(16): 3682..

[7] Motter A E, Lai Y C. Cascade-based attacks on complex networks [J]. Physical Review E, 2002, 66(6): 065102.

[8] Wieland A, Marcus Wallenburg C. Dealing with supply chain risks: Linking risk management practices and strategies to performance [J]. International Journal of Physical Distribution & Logistics Management, 2012, 42(10): 887-905.

[9] PENG Xing-zhao, YAO Hong, ZHANG Zhi-hao, DU Jun. Research on cascading invulnerability of scale-free networks under node-based-attack. Systems Engineering and Electronics, 2013, 35(9): 1974-1978.

[10] Moreno Y, Gómez J B, Pacheco A F. Instability of scale-free networks under node-breaking avalanches [J]. Europhysics Letters, 2002, 58(4): 630.

[11] Motter A E, Lai Y C. Cascade-based attacks on complex networks [J]. Physical Review E, 2002, 66(6): 065102.

[12] Wang J, Rong L, Zhang L, et al. Attack vulnerability of scale-free networks due to cascading failures[J]. Physica A: Statistical Mechanics and its Applications, 2008, 387(26): 6671-6678.

[13] REN Jun Liang, SHEN Mao Xing, TONG Rui, et al. Study of reducing size of cascading failures in scale-free network [J]. Computer Engineering and Applications, 2011, 47（33）: 82-84.

[14] MA Yi hua, KANG kai. Model for Cascading Failures in Complex Networks Based on Non-linear and Surplus Capacity [J]. Journal of System Simulation, 2013, 5: 003.

[15] Au, Chun Yin, Fan Yan, KAIHAU YEUNG. Congestion model for cascading failures in complex networks. Proceedings of the 9th WSEAS international conference on Applied informatics and communications [J]. World Scientific and Engineering Academy and Society (WSEAS), 2009.

[16] Wang J, Rong L, Zhang L. A model for cascading failures in complex networks with a tunable parameter [J]. Modern Physics Letters B, 2009, 23(10): 1323-1332.

[17] Wang J. Robustness of complex networks with the local protection strategy against cascading failures [J]. Safety Science, 2013, 53: 219-225