Research on Defense Model of Cascading Failures in Complex Information System Networks

Xi Chen[1,a], Qi Li[2]

[1,2]Beijing University of Posts and Telecommunications, Beijing 100876, China.

[a]572214342@qq.com

Keywords: Complex information system network; Emergency flow-limiting model; Cascading failure defense; Module-deleting model; Simulation analysis

Abstract. With the improvement of social information network, the information infrastructure confronts with increasing security threats. Governments and security groups are reinforcing research on the complex information systems vulnerabilities and especially the network vulnerabilities. Among them, the defense of network cascading failures is one of the most important safety issues in complex network. This paper made a research on the defense mechanism against cascading collapse effect in communication networks and proposed a defense model based on emergency flow-limiting mechanism. And by using three sample networks in simulation experiments, the plan has been proved working well in controlling and defensing cascading collapse phenomenon appearing in communication networks. At the same time, we conducted some simulating researches and analyses on defense plan of deleting the modules with lower centralization degree. By comparison, we find defense model with emergency flow-limiting mechanism has a wider application scope and higher efficiency, while costing less, providing prominent theoretical support to prevention and control of network cascading failures.

Introduction

In many classic load - capacity models of network cascade dynamics, it is often assumed that once the load in the network nodes or sides exceeds their maximum capacity, the corresponding nodes or sides will crash out of action, resulting in redistribution of network loads, and triggering cascading effects.

In terms of emergency strategies of cascading reaction, taking characteristics of four different network models into account, Buzna[1,2] investigated the impact of the dynamics characteristics of the node itself (such as adaptability , status, etc.) on network disaster spreading by using weights neural network model , and discussed the effectiveness of six coping strategies and optimal strategy in detail. A lot of control and prevention strategies for cascade behavior have been proposed on how to get the best ability to resist cascade reaction by limited resources[3,4,5], OuYang and others[6] study the cascade dynamics of a complex system with redundant resources by using the node dynamics equations in response to disasters and accidents in infrastructure networks, and compare the effectiveness of different resource allocation strategies respectively.

In this paper, starting from this idea, we propose a defense model based on emergency flow-limiting mechanism and prove that it can solve cascade crash in communication networks better by using three kinds of communication backbone networks in simulation. Meanwhile, this paper will have a simulation study and comparison on another early defensive plan.

Defense Model Based on Emergency Flow-limiting Mechanism

First, forming new network cascade dynamics model possessing emergency handling mechanism and taking various network side-attacking strategies for reference, this paper researches into emergency handling mechanism of failure spread[7].

Supposing there are N nodes and N_e sides in a non-oriented, weighted network G, and defining network adjacency matrix as $A=(a_{ij})_{N\times N}$, if there is side connecting Node i and Node j, then a_{ij}=1 ,or a_{ij}=0. Also, suppose weight of Side e_{ij} as w_{ij}.

As for cascade dynamics model construction of network that has emergency handling mechanism, we set out mainly from the below 3 aspects: definition on initial loads of sides in network ,and definition on the relation of initial loads of sides and maximum capacity of sides, and dynamic evolution mechanism of side load redistribution process after sides are attacked[8].

Definition on Initial Load $L_{ij}(0)$ of Link e_{ij}. In weighted network G, at Time t, load $L_{ij}(t)$ of Side e_{ij} can be defined as the amount of the shortest paths via Side e_{ij}. When t=0, which means time before attack, initial load of Side e_{ij} is $L_{ij}(0)$.

Definition of Maximum Capacity C_{ij} of Link e_{ij}. Suppose C_{ij} is the maximum load that Side e_{ij} is able to handle (also the maximum capacity) in the network, and it's to be directly proportional to initial load $L_{ij}(0)$ of Side e_{ij}. Their relation is as follow:

$$C_{ij} = (1+\alpha)L_{ij}(0) \tag{1}$$

Adjustable coefficient $\alpha>0$ above stands for tolerate factor.

Definition of Emergency Handling Start Point. We can divide network links in cascading collapse model into 3 kinds: load that is below $L_{ij}(0)$, above $L_{ij}(0)$ but below or equal to C_{ij}, and is above C_{ij}; The first one is normal status, the second congestion status and the third invalid one. The conditions needed for Link e_{ij} to start emergency mechanism in a congestion status can be represented by Load threshold C_{ij}^{*} as:

$$C_{ij}^{*} = (1+m\alpha)L_{ij}(0)\ m\in(0,1) \tag{2}$$

Meanwhile, we set that only when Link e_{ij} is in congestion and load exceeds threshold C_{ij}^{*}, emergency mechanism become effective. If link load does not exceed C_{ij}^{*}, there will be no interference from emergency mechanism.

Definition of Emergency Handling Resources. Supposing emergency handling is realized by reducing link loads, the total of emergency handling resources available is τ, and the maximum of emergency handling resources available to Link e_{ij} according to its weight in network is τ_{ij}, we get:

$$\tau_{ij} = \tau w_{ij} / \sum w_{ij} \tag{3}$$

Among which, w_{ij} stands for emergency resources weight allocated to Link e_{ij}, and variable parameter τ for the total of external resources entered network. By changing value ofτ, resources entered network can be controlled.

Network Load Redistribution Process. Assuming that at Time t, when some sides is collapsing, temporary load on e_{ij} is $L'_{ij}(t)$. If $L'_{ij}(t)$ exceeds its threshold C_{ij}^{*}, emergency handling will intervene and distribute Side e_{ij} with certain proportion of emergency resources .At that moment, load of Side e_{ij} decreases, and changes into $L_{ij}(t)$ at next moment. The definition is as follow:

$$L_{ij}(t)=\begin{cases} L'_{ij}(t) & if \quad L'_{ij}(t) < C_{ij}^{*} \\ L'_{ij}(t)-\beta\tau_{ij} & if \quad C_{ij}^{*} \le L'_{ij}(t) \le C_{ij} \\ L'_{ij}(t)-\tau_{ij} & if \quad C_{ij} < L'_{ij}(t) \end{cases} \tag{4}$$

Among which,

$$\beta = \frac{L'_{ij}(t)-C_{ij}^{*}}{C_{ij}-C_{ij}^{*}} \tag{5}$$

Thus, we give definition to normal status $L'_{ij}(t) < C_{ij}^{*}$, congestion status $C_{ij}^{*} \le L'_{ij}(t) \le C_{ij}$ and overloaded, collapsing status $C_{ij} < L'_{ij}(t)$.

Link Cascading Failures Defense Emergency Procedures. According to analyses above, we get the following link cascading failures defense emergency procedures:

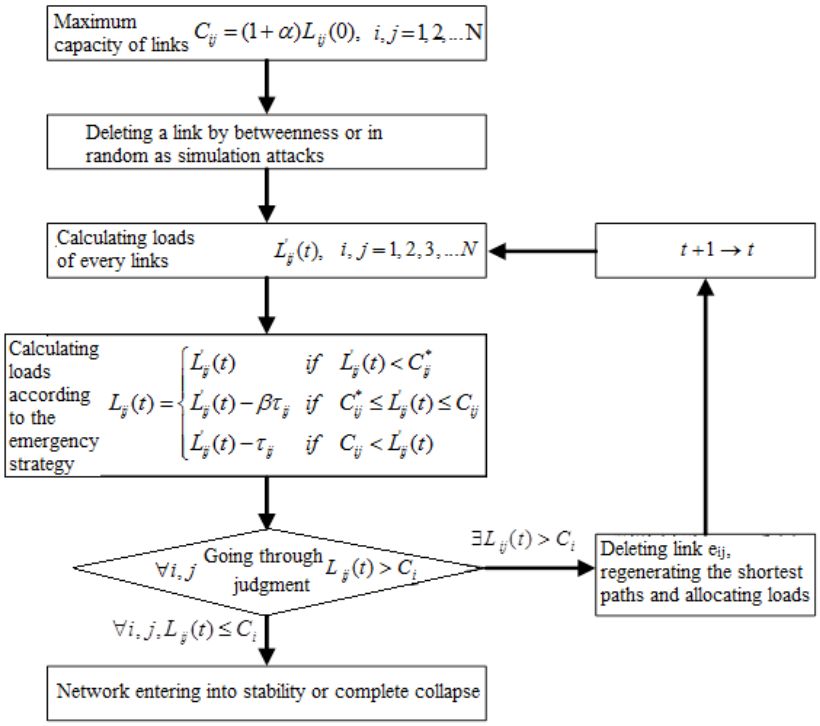

Figure. 1 Link cascading failures defense emergency procedures

The following procedures show link cascading failures: When a flow in the network is deleted, loads will be reallocated in the whole network, meanwhile, emergency mechanism loads Link e_{ij} with resources at Time t according to scheduled tactics. If the load amount of e_{ij} still exceeds its maximum capacity, the side will collapse, causing a new turn of load reallocation and cascade reaction. The iterative process will last until no more new link failures occurs, and network come into stability or a complete collapse .At this time, cascading effect will stop[9].

Simulation Analysis of Cascading Failures in Emergency Mechanism. Next, through simulation, we will take 3 networks as examples to analyze their cascading failures occurring in emergency handling mechanism. Here, we take α=0.1, and then compare vertically cascading failures of INTERNET2, CRNET and CERNET2 under different stimulation emergency resource situations. The following is comparison of results about attack on betweenness nodes:

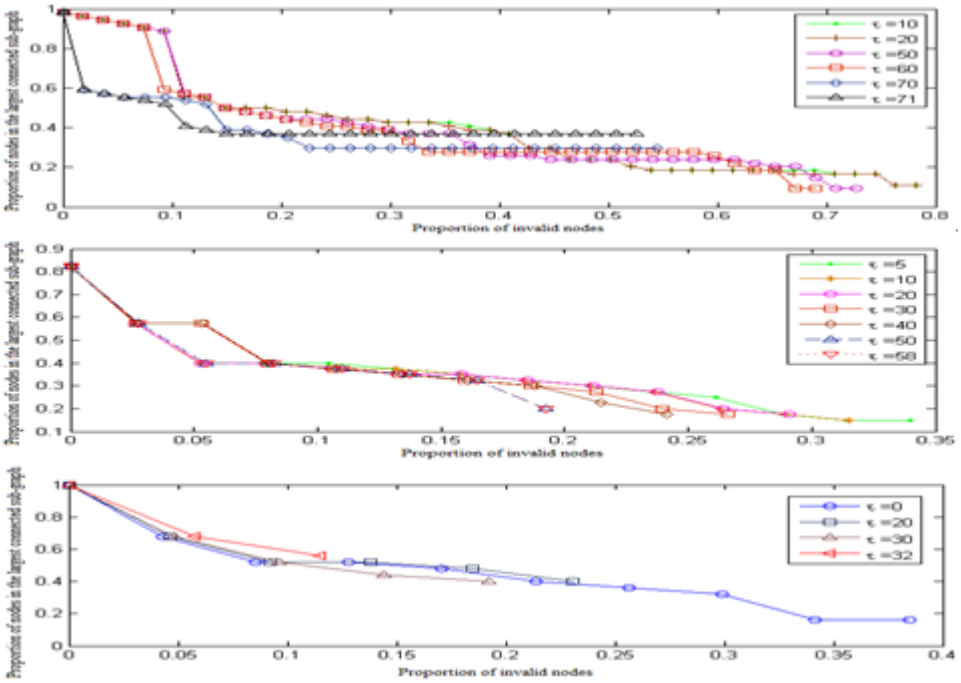

Figure. 2 Simulation attack on nodes of INTERNET2 / CRNET / CERNET2 using betweennesses under emergency defense program

According to figures above, in the three networks, with the increase of emergency resources, proportion of invalid nodes and scale of cascading failures are decreasing, while node proportion of maximum connected sub-graph are increasing; But node proportion in maximum connected sub-graph decreases quite fast, with the increasing of invalid nodes, which indicates links that plays an significant role in maintaining network connectivity collapse too early in cascading failures. The phenomenon can be illustrated as follows: In cascading failures, when emergency resources are allocated evenly into different links, they act as a protection of links with lower betweenness. On the contrary, overload is more likely to occur in links with higher betweenness, resulting in early link collapse.

Low-centricity-module-deleting Defense Model

Model Analysis of Module-deleting Program. Aiming at cascading effect defense, Adilson E. Motter[10] proposes controlling the scale of cascading failures by selectively deleting some nodes with lower centricity ,after initial nodes fail and before cascading failures occur, to ensure that most parts of network are connected. This model divides cascading failures into two stages. In Stage 1, where initial nodes become invalid, has p percent of nodes failed; In Stage 2, cascading spread stage, other nodes are effected and become invalid.

Perform simulation experiments as the following 5 projects. Node-deleting program 1: Deleting by Δ_i value of nodes, starting from small one to large one; Node-deleting program 2: Deleting according to node tightness $\bar{D}_i^{-1}$, starting from small one to big one; Node-deleting program 3: Deleting by node capacity L_i, also from small to large; Node-deleting program 4: Deleting by node degree, starting from low to high; Link-deleting program: Deleting by loads of links.

Simulation Experiment. First, generating scale-free networks with exponent γ=3 in power function, in which, node amount N=5000, minimum node degree K_0=2, and initial invalidity rate p=0.001. Result is as Figure 3(A) shown:

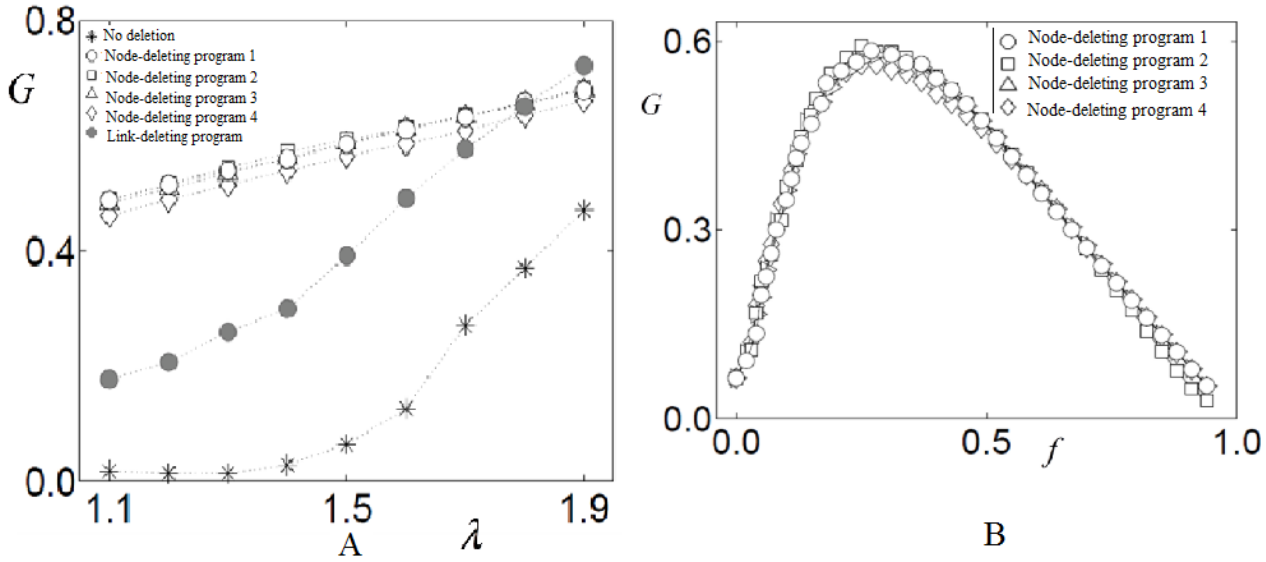

Figure. 3 Comparison of cascading failure defense program

$\lambda=1+\alpha$ stands for capacity coefficient, $G=N'/N$ node proportion and N' node number of maximum connected sub-graph .From the figure above, we can see after using defense mechanism, the value of G increases and network capacity against cascading failures is enhanced. Also, we find overall defense effects of the 4 node-deleting programs are better than that of link-deleting program. When, node-deleting programs increase proportion of connected nodes by 60%, while link-deleting program 30%.

As Figure 3(B) shown, f stands for proportion of nodes deleted on purpose, and G for node proportion in maximum connected sub-graph. By simulating cascade process, we can find the connection between proportion of nodes deleted and connectivity. From the figure above, we can see effects of the four node defense programs are similar. When f <0.4, connectivity increases with the increase of proportion of node deleted and most losses on connectivity is caused by cascading effect; When $f \approx 0.4$, cascading effect is under controlled, and only a small part of losses are causing by defensive deletion; When $f \geq 0.4$, the curve generally conform to $G=1-f$, and there are only losses causing by defensive node deletion.

Comparison of Module-deleting Plan and Emergency Flow-limiting Plan. Simulation experiments show that the method of deleting smaller nodes (or links) with lower centralization degree is effective, but it has shortcomings compared with emergency flow-limiting plan. First, though this method deletes node (or link) with lower centricity and smaller capacity, the amount of network flows cut is large. And since the level of flows cut each time is equal to the total cutting amount$\tau$of emergency plan and after deleting one more module, the flow will multiply than that in emergency flow-limiting plan, which will bring greater impact to the network topology and efficiency. Second, the flow re-allocation process will increase the load on the information network structure, which may lead to a new cascading collapse under the most unfavorable network. This kind of bad effect will never happen to the emergency flow-limiting plan. Therefore, emergency flow-limiting plan has more advantages.

Conclusion

After doing researches on defense mechanism of the communication network cascading collapse effect, this paper proposed an emergency plan based on flow control and tested it using 3 example networks .Comparing with plan of deleting modules with lower centralization degree, this plan has no side effects, and can control and defense against network cascading failures more efficiently.

References

[1] Buzna L., Peters K., Ammoser H., et al., Efficient response to cascading disaster spreading, Phys. Rev. E, 75, 2007, 056107.

[2] Peters K., Buzna L., Helbing D., Modelling of cascading effects and efficient response to disaster spreading in complex networks, Int. J. Critical Infrastructures, 4(1/2), 2008.

[3] Jacob Aron，The cyberweapon that could take down the INTERNET，NewScientist 11 February 2011

[4] Li P., Wang B.-H., Sun H., et al., A limited resource model of fault-tolerant capability against cascading failure of complex network, Eur. Phys. J. B, 62, 2008, pp. 101-104.

[5] Wang B., Kim B.J., A high-robustness and low-cost model for cascading failures, Europhysics Letters, 78, 2007, 48001.

[6] Ouyang M., Fei Q., Yu M.H., et al., Effects of redundant systems on controlling the disaster spreading in networks, Simulation Modelling Practice and Theory, 17, 2009, pp. 390-397.

[7] Dou B.-L., Wang X.-G., Zhang S.-Y., Robustness of networks against cascading failures, Physica A, 389, 2010, pp. 2310-2317.

[8] Wang J.W., Rong L.L., Cascade-based attack vulnerability on the US power grid, Safety Science, 47, 2009, pp. 1332-1336.

[9] http://www.internet2.edu/network/

[10]Motter A.E., Cascade control and defense in complex networks, Phys. Rev. Lett., 93, 2004, 098701.