Model of Cascading Failures for Communication Networks

Lei Zhu, Xiaochen Liu*, Lu Yu, Xinrong Wu
Collage of Communications Engineering, PLA University of Science and Technology, Nanjing, China.

* Corresponding author. Tel.: 8613814079219; email: liuxiaochenyt@163.com
Manuscript submitted October 9, 2015; accepted January 7, 2016.
doi: 10.17706/ijcce.2016.5.5.302-310

Abstract: Communication networks play such a critical role in modern society that any failures in these networks are intolerable. In this study, we focus on the influence of network congestion and build a model to study the dynamics of cascading failures in communication networks. Investigation of the relationship between the initial allocation of efficiency among edges and the damage caused by cascading failures shows that a higher initial efficiency may lead to more severe consequence in case of cascading failures. We also investigate the influence of the size of the router's buffer. Because the correct buffer size can alleviate network congestion to some extent, it is able to enhance the robustness of the network against cascading failures.

Key words: Cascading failures, communication networks, network congestion, network efficiency, buffer size.

1. Introduction

Communication networks including telephone network, computer network, and cellular networks as well as the Internet, are an essential part of the current social infrastructure. With the rapid development of information technology, both the scale and complexity of communication networks have surpassed expectation. To study these kind networks, the theory of complex network was proposed [1], [2]. Given their importance, the robustness of communication networks has attracted much attention in recent years. Previous studies [3], [4] have found that cascading failures are very common in complex networks. Owing to the heterogeneity of the network and the interaction of different parts, even a single failure can cause the entire network to collapse. For example, in October 1986, during the first documented congestion-induced Internet collapse, the speed of the connection between the Lawrence Berkeley Laboratory and the University of California at Berkeley, which are located only 200 m apart, dropped by a factor of 100 [5], [6]. Because society is becoming increasingly reliant on communication networks, research on the causes and dynamics of cascading failures in complex networks has become quite meaningful.

In recent decades, a great deal of literature on cascading failures has been published. Albert *et al*. [7] found that scale-free networks are highly robust against random failure; however, in case of a deliberate attack against highly connected nodes, these networks are extremely vulnerable. Motter and Lai [8] introduced the concept of cascading failure and proposed the famous ML model, which is quite enlightening for later research. Considering that the removal of overloaded nodes does not correspond to many real-life situations, Crucitti *et al*. [9] constructed the CML model. In this model, when a node is overloaded, the transmission efficiency of links associated with this node decreases, instead of disconnecting the nodes. However, the way transmission efficiency decreases does not reflect the actual situation in communication

networks. Taking account of the weights of edges, Baharan *et al*. [10] improved the previous models by finding the optimal weight of each edge in an effort to mitigate cascading failures. Using a random walk model, Kishore *et al*. [11] suggested a revision of the design principles to handle extreme events smoothly.

Most current research focuses on cascading failures in a universal complex network representing different kinds of actual networks. In fact, there is no actual network with the identical characteristics. In this study, we map a communication network to a complex network and redefine the elements of complex networks based on specific features in practice. Each node denotes a router for its critical characteristic in communication networks. Each node is allocated a data forwarding rate and buffer size, both of which have been ignored in previous research. An edge characterizes the connection relationship between routers, while the weight of an edge reflects its transmission efficiency. In different networks, the reasons for cascading failures may be diverse. For an electricity network, an overload of power causes the equipment to fail, whereas, in communication networks, we focus on the impact of traffic congestion. When a component fails, its load shall be redistributed over the entire network. Additional load can cause a router to be unable to handle the packets received, which leads to a higher packet loss rate at the buffer. This failure transfers from one router to another, resulting in the collapse of the entire network. In this study, we investigate different factors related to the robustness of networks against cascading failures to find various mitigation strategies.

In Section 2, we abstract a communication network into a complex network and redefine its components. In Section 3, we study the dynamic behavior of networks in the presence of cascading failures. Simulations and an analysis of the results are outlined in Section 4, while our conclusions are presented in Section 5.

2. Model of a Communication Network Based on Complex Network

Communication networks including different kind of networks can provide an information dissemination service for users at different locations. A communication network system consists of different physical devices and a variety of network protocols. Because the routers responsible for storing and forwarding data packets play a central role in the network, research on the interaction between routers is crucial for maintaining network performance. The substantial development of communication networks with few predictable plans has led to the very large scale of, and extremely complex connections between, routers. Based on empirical research, Goldenberg *et al*. [12] found small-world and scale-free properties in communication networks, thereby laying a solid foundation for the promotion and application of complex network theory.

Assuming a communication network such as an autonomous system (AS) of the Internet comprising a vast number of routers and other equipment, we abstract it into a graph, $G(V,E)$. Here, V is the set of nodes representing the routers in the network, and E is the set of edges describing the physical connections between routers. In our model, we assume that the network is a BA scale-free network [2]. Since a router has the function of storing and forwarding, we depict node i in V with some parameters describing this characteristic. We define the forwarding load l_i of node i, denoting the amount of data needed to be forwarded per unit time. A router also has an upper limit on the forwarding rate, expressed as the forwarding capacity c_i. If the forwarding load surpasses its forwarding capacity, some packets are stored in the buffer if there is enough space. We denote the buffer size of router i as b_i. Due to economic and technical limitations, the forwarding capacity and buffer size are limited. Thus, it is natural to assume that these are proportional to its initial forwarding load l_{i0} [8]:

$$c_i = (1+\alpha)\cdot l_{i0} \tag{1}$$

$$b_i = (1+\beta)\cdot l_{i0} \tag{2}$$

where α denotes the forwarding tolerance, and β is the buffer tolerance, both of which are positive constants.

We define the transmission efficiency of link e_{ij} between nodes i and j as λ_{ij} representing the amount of data transmitted correctly by link e_{ij} per unit time. According to [6], [13], for the initial transmission efficiency we have $\langle \lambda_{ij0} \rangle \propto (k_i k_j)^{\theta}$, where k_i is the degree of node i, and θ is a constant. Considering the vast number of edges in a network and referring to the law of large numbers, we can safely assume that the distribution of λ_{ij0} obeys the normal distribution. That is,

$$F(\lambda_{ij0} > x) = \int_x^{+\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{-(x-\xi(k_i k_j)^{\theta})^2/(2\sigma^2)} dx \tag{3}$$

where $F(\cdot)$ is the probability that λ_{ij0} has a larger value than x, σ is the standard deviation, and ξ is a tunable constant. The process of modeling the complex network is shown in Fig. 1, and the main parameters have been marked in the figure.

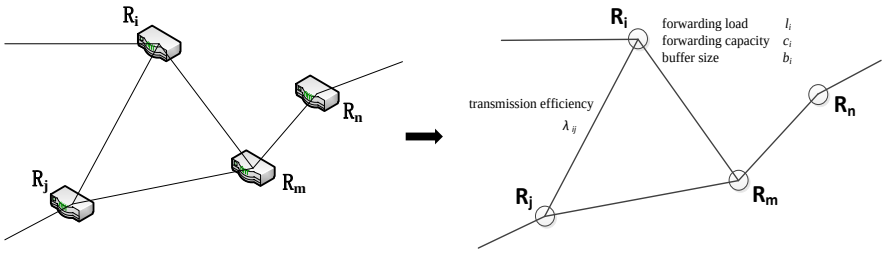


Fig. 1. Process of modeling communication networks based on a complex network. We focus on routers in a communication network and define some parameters to describe the routers and links.

Let ε_{sd} be the time taken to transfer a packet from source node s to destination node d. P_{sd} is the shortest path along which the time for data transmission is minimal. Thus,

$$\varepsilon_{sd} = \sum_{e_{ij} \in P_{sd}} \frac{1}{\lambda_{ij}} \tag{4}$$

In our model, we not only build the network topology, but also define some parameters describing the nodes and links. Later, we investigate the influence of these parameters.

3. Dynamics of Cascading Failure

Many current models of cascading failures tend to remove broken-down component whose load has exceeded its capacity. However, in practice, a router that cannot forward all the packets received timeously should not be hastily removed. In more general cases, the overloaded router keeps working, but at a lower efficiency. Various studies [8], [14] have considered this problem, although they merely roughly describe the decline in efficiency. In our model, we study the decline in efficiency of routers caused by overloading and its adverse impact on the network. Our assumptions for the model are the following:

1) Each router in the network sends packets at the same rate;
2) Updates of the routing table are rapid enough;
3) The sender takes no congestion control protocol.

According to assumption 1), the data forwarding rate of a router is proportional to the number of shortest paths passing through it. Thus, the forwarding load l_i of node i can be set as its betweenness centrality [15], [16].

From (2), we can see that during normal operation of the network, no router is overloaded, and we can set a proper β to ensure that the buffer has enough space for the packets. We define the network efficiency $E(G)$, measuring the overall operation status of the network [17] as

$$E(G) = \frac{1}{N(N-1)} \sum_{s \neq d \in V} \frac{1}{\varepsilon_{sd}} \tag{5}$$

where N is the number of nodes in the network. Obviously, a larger $E(G)$ indicates stronger transmission capacity of the network, reflecting a better operation status of the communication network.

If for some reason (equipment failure, human damage, etc.) one or more nodes go breakdown at time t, the failed component is removed from the network. After this failure, the routing table of the network is updated according to the routing algorithm, which means that the forwarding loads of the remaining nodes in the network are redistributed. According to assumption 2), the time required for redistribution is small. For node i, the change in forwarding load is denoted by $\Delta l_i(t)$ and the original load at t is $l_i(t)$. If $l_i`(t) = \Delta l_i(t) + l_i(t) > c_i$, node i becomes overloaded. In this situation, i fails, but is not removed from the network. The node or router has to receive more data than its forwarding capacity which inevitably will lead to buffer overflow. In fact the data discarded by the router wasted the transmission resource of the links which transferred then. We can conclude that the amount of data transmitted correctly by these links got smaller because of the overload, it meant that the transmission efficiency decreased accidentally. The router usually abandons the data transferred by every link connected with it, so it`s reasonable to presume that the transmission efficiency of all the links connected with the overloaded router decrease in the same way. That is,

$$\lambda_{ij}(t+1) = \lambda_{ij}(t) \cdot (1 - p_i(t)) \tag{6}$$

$\lambda_{ij}(t)$ is the transmission efficiency of link e_{ij} and $p_i(t)$ is the decline factor caused by node i at time t, which is discussed in a subsequent section.

In the traditional CML model [8], $p_i(t)$ is proportional to the quotient of the load and capacity of node i. However, in communication networks, this assumption does not accurately describe the efficiency decline of links. In a router, packets received are stored temporarily in the buffer. If the rate of receiving data exceeds the capacity to forward packets, which means the forwarding load is greater than the forwarding capacity, the buffer will become full and newly received packets will be dropped. There are many queue management algorithms for managing a router's buffer, DropTail as the most naive is very widely used in communication networks. Under the DropTail mechanism all the data arriving at the router when buffer gets full will be abandoned. This queue management can be modeled by queuing theory [18], [19].

In this model we assume that all packets contain the same number of data bytes. Given that the forwarding load of router i is $l_i(t)$, the number of packets received per unit time is,

$$\lambda_{\text{queue}} = \frac{l_i(t)}{L} \tag{7}$$

where L is the number of bytes per packet contains.

When a router gets overloaded, it's natural to think it is doing its best work. In this circumstance, the forwarding speed of packets is,

$$u_{\text{queue}} = \frac{c_i}{L} \tag{8}$$

The buffer size of router i is b_i which means it can store as many as b_i packets at a time. When a packet arriving at or leaving the router obeys the Poisson process, based on the $M/M/1/k$ queuing theory model [20], [21], the probability of the system get empty is,

$$p_o = \frac{1-\left(\frac{\lambda_{\text{queue}}}{u_{\text{queue}}}\right)}{1-\left(\frac{\lambda_{\text{queue}}}{u_{\text{queue}}}\right)^{b_i+1}} \tag{9}$$

And the probability of the system get full is,

$$p_{\text{full}} = \left(\frac{\lambda_{\text{queue}}}{u_{\text{queue}}}\right)^{b_i} \quad p_0 = 1-\frac{1-\left(\frac{l_i(t)}{c_i}\right)^{b_i}}{1-\left(\frac{l_i(t)}{c_i}\right)^{b_i+1}} \tag{10}$$

When the router's load is smaller than its capacity, we ignore the packet loss rate. Thus, $p_i(t)$ is calculated as

$$p_i(t) = \begin{cases} 0 & l_i(t) \le c_i \\ 1-\dfrac{1-\left(\frac{l_i(t)}{c_i}\right)^{b_i}}{1-\left(\frac{l_i(t)}{c_i}\right)^{b_i+1}} & l_i(t) > c_i \end{cases} \tag{11}$$

At time t+1, the routing table is updated according to the new efficiency of the edges. This process continues until the network stabilizes or collapses completely.

4. Simulations and Analysis of Results

Many researchers find that the topology of Internet has the features of complex network such as small world and scale-free [22]-[24]. In our simulations we built a B-A scale-free network [2]. The nodes of network stand for routers in Internet and the edges stand for the links between routers.

A communication network may experience random failures or a deliberate attack, which is more likely to affect critical nodes at runtime. We simulate these two kinds of failure in our model. For random failures, we chose 10 nodes arbitrarily as the initial failed components. For the deliberate attack, we found the node with the largest betweenness centrality to disable it. From Fig. 2 we can see that a deliberate attack does more damage to the network. This result is consistent with that of Motter [8].

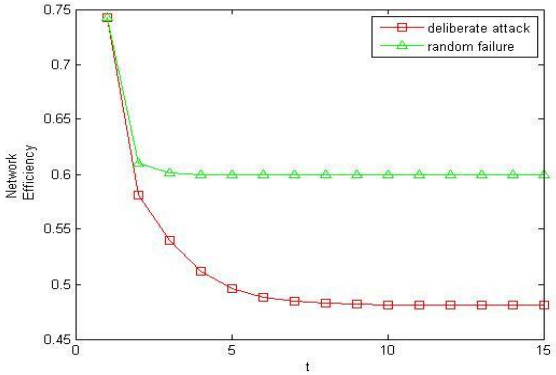


Fig. 2. Network efficiency change over time for random failure and deliberate attack. The network is a B-A scale-free network with 1000 nodes. In this experiment, we set α to 0.2, β to 20 and ξ to 1. The data used are averages over 10 realizations.

We defined the transmission efficiency of an edge in Section 2. If the overall initial transmission efficiency (the sum of the transmission efficiency of all edges) is fixed as Ψ, parameter θ influences the initial allocation of efficiency among edges. That is,

$$\lambda_{ij0}` = \frac{\lambda_{ij0}}{\sum_{e_{mn} \in E} \lambda_{mn0}} \cdot \Psi \tag{12}$$

where $\lambda_{ij0}`$ is the renormalized initial transmission efficiency of edge e_{ij} and λ_{ij0} is defined in Section 2.

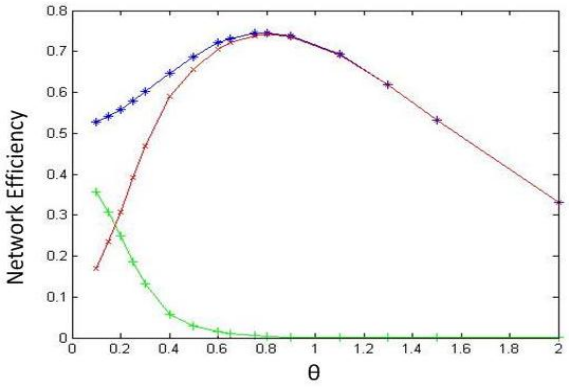


Fig. 3. Network efficiency as a function of θ for the initial, final, and declined network efficiency on a B-A scale-free network with 1000 nodes. In this experiment, we set α to 0.2, β to 20 and ξ to 1. Data used are averages over 10 realizations. The blue, green and red lines show the initial, final, and declined network efficiency, respectively.

Fig. 3 shows that the initial network efficiency increases with the value of θ, but it declines after the extreme point at about θ = 7.3. As θ increases, the network becomes more heterogeneous, which leads to a more adverse impact of the deliberate attack. The network goes collapse when θ results in the largest initial network efficiency. Thus, we need to set the correct value of θ to make the network run efficiently, thereby enhancing the robustness of the network against cascading failures.

In Fig. 4, we report the final network efficiency after the cascading failure as a function of the forwarding tolerance parameter α. We begin our simulation with three different values for the buffer tolerance parameter β. This shows that for the first buffer tolerance value, the final network efficiency increases as

the forwarding tolerance first increases and eventually becomes stable. This means that if we improve the forwarding rate of the routers in the communication network, the network becomes more robust. This is consistent with our intuition. Moreover, for different values of β, the final network efficiency becomes consistent if α is large enough. That is, a higher forwarding rate can compensate for the lack of buffer sizes in routers.

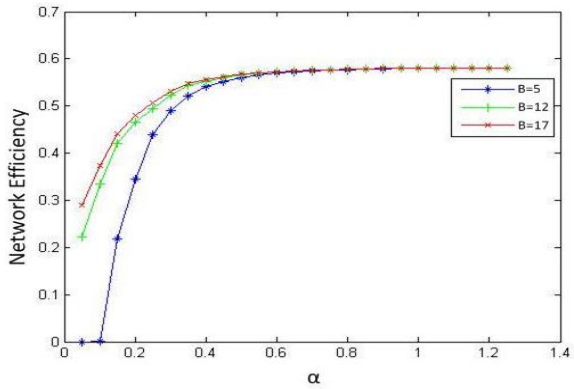


Fig. 4. Network efficiency as a function of α for different buffer tolerance parameter values on a B-A scale-free network with 1000 nodes. The data shows averages over 10 realizations.

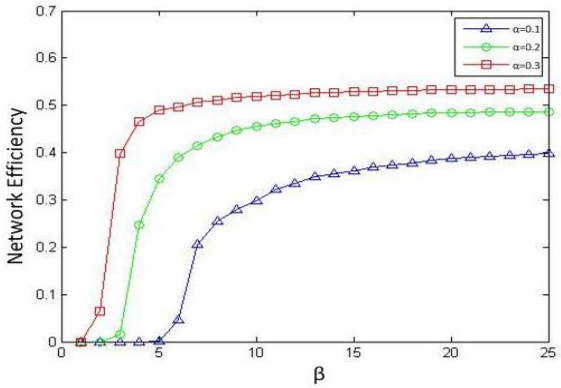


Fig. 5. Network efficiency as a function of β for varying forwarding tolerance parameters values on a B-A scale-free network with 1000 nodes. Data shows averages over 10 realizations.

Fig. 5 shows the changes in the final network efficiency corresponding to the tolerance parameter β. We can see that a larger tolerance parameter reduces the adverse effect of cascading failures. It is impressive to a phase change during the process of increasing parameter β. We can explain this phenomenon through (10). From this equation, the blocking probability p_{full} increase very fast when the argument b_i is relatively small, and the growth trend gets quite slow when b_i is large enough. In fact, if α is relatively large, the variation trend of p_{full} will become sharper. It is coincident with Fig. 5. In the whole network, the phase change happens if the size of buffer is very influential to packet loss rate which means that the value of b_i is proper. On the S-shaped curve, an optimal β can be found for maximum effect. Moreover, we observe that a larger forwarding tolerance parameter helps the curve of β converge to a larger value. In practice, we cannot increase the forwarding rate of routers without limitation. However, faced with a low forwarding rate, we can increase the size of the buffer to enhance the robustness of the network. This observation is useful for network planners.

5. Conclusion

We created our model to study cascading failures in communication networks. In our model, we

considered the critical role of congestion and noticed the effect of buffer length for routers, something that has previously been ignored. Various parameters were investigated in this paper. The edge efficiency parameter θ not only influences the initial allocation of efficiency among edges, but also the decline in network efficiency. For global load redistribution, there is no optimal θ for the robustness of a network, which means that the smaller θ is always helpful the robustness of networks. The forwarding tolerance parameter and buffer tolerance parameter influence the final network efficiency in different ways. Although larger values for both are beneficial for the network, a sufficiently large forwarding tolerance parameter can negate the influence of the buffer tolerance parameter, although the reverse is not true.

Our result can help enhance the reliability of communication networks. Users can choose the proper initial allocation of efficiency and set adequate forwarding capacity or buffer size for routers in an attempt to mitigate cascading failures.

References

[1] Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of 'small-world' networks. *Nature*, *393(6684)*, 440-442.

[2] Barabási, A. L., & Albert, R. (1999). Emergence of scaling in random networks. *Science*, *286(5439)*, 509-512.

[3] Van Eeten, M., *et al*. (2011). The state and the threat of cascading failure across critical infrastructures: The implications of empirical evidence from media incident reports. *Public Administration*, *89(2)*, 381-400.

[4] Zhu, Y., Yan, J., *et al*. (2014). Revealing cascading failure vulnerability in power grids using risk-graph. *IEEE Transactions on Parallel and Distributed Systems*, *25(12)*, 3274-3284.

[5] Floyd, S., & Jacobson, V. (1993). Random early detection gateways for congestion avoidance. *IEEE/ACM Transactions on Networking, 1(4)*, 397-413.

[6] Yazdani, N., Araújo, N. A. M., *et al*. (2013). Towards designing robust coupled networks. *Scientific Reports*.

[7] Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. *Nature*, *406(6794)*, 378-382.

[8] Motter, A. E., & Lai, Y. C. (2002). Cascade-based attacks on complex networks. *Physical Review E*, *66(6)*.

[9] Crucitti, P., Latora, V., & Marchiori, M. (2004). Model for cascading failures in complex networks. *Physical Review E*, *69(4)*, 045104.

[10] Mirzasoleiman, B., Babaei, M., Jalili, M., *et al*. (2011). Cascaded failures in weighted networks. *Physical Review E*, *84(4)*, 046114.

[11] Kishore, V., Santhanam, M. S., & Amritkar, R. E. (2011). Extreme events on complex networks. *Physical Review Letters*, *106(18)*, 188701.

[12] Liu, Y. Y., Slotine, J. J., & Barabási, A. L. (2011). Controllability of complex networks. *Nature*, *473(7346)*, 167-173.

[13] Wei, D., Deng, X., Zhang, X., Deng, Y., & Mahadevan, S. (2013). Identifying influential nodes in weighted networks based on evidence theory. *Physica A: Statistical Mechanics and its Applications*, *392(10)*, 2564-2575.

[14] Ash, J., & Newth, D. (2007). Optimizing complex networks for resilience against cascading failure. *Physica A: Statistical Mechanics and its Applications*, *380*, 673-683.

[15] Freeman, L., (1977). A set of measures of centrality based on betweenness. *Sociometry*, *40(1)*, 35-41.

[16] Anthonisse, J, (1971). The rush in a directed graph. Report BN/71, Stichting Mathematisch Centrum, Amsterdam, Netherlands.

[17] Wang, Q., Su, T. P., Zhou, Y., Chou, K. H., Chen, I. Y., Jiang, T., & Lin, C. P. (2012). Anatomical insights into disrupted small-world networks in schizophrenia. *Neuroimage*, *59(2)*, 1085-1093.

[18] Saaty, T. L. (1961). *Elements of Queuing Theory*. New York: McGraw-Hill.

[19] Vickrey, W. S. (1969). Congestion theory and transport investment. *The American Economic Review*, 251-260.

[20] Brownlee, K. A. (1965). *Statistical Theory and Methodology in Science and Engineering*. New York: Wiley.

[21] Hamadneh, N., Murray, D., Dixon, M., & Cole, P. (2012). Dynamic weight parameter for the random early detection (RED) in TCP networks. *International Journal of New Computer Architectures and Their Applications*, *2(2)*, 342-352.

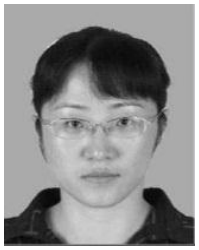
[22] Stewart, M., Loschen, W., & Kass-Hout, T. (2013). Enabling ESSENCE to process and export meaningful use syndromic surveillance data. *Online Journal of Public health Informatics*, *5(1)*.

[23] Shavitt, Y., & Zilberman, N. (2012). Geographical internet pop level maps. *Proceedings of 4th International Workshop of Traffic Monitoring and Analysis* (pp. 121-124).

[24] Çetinkaya, E. K., Broyles, D., Dandekar, A., Srinivasan, S., & Sterbenz, J. P. (2013). Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: A simulation-based approach. *Telecommunication Systems*, *52(2)*, 751-766.

Lei Zhu was born in 1973. Dr. Lei Zhu is a professor in PLA University of Science and Technology. His research interests are network planning and management, data processing and information service.

Xiaochen Liu was born in 1990. He obtained his bachelor's degree in PLA University of Science and Technology and now he is pursuing the postgraduate degree. His research interests are network planning, management, and complex network.



Lu Yu was born in 1974. She received a PhD degree and is an adjunct professor in PLA University of Science and Technology. Her research interests are data mining and computer network.

Xingrong Wu was born in 1970. She obtained her postgraduate degree from PLA University of Science and Technology. Her main research interest is network planning and management.