Reliability Engineering and System Safety 117 (2013) 1–8

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Research on robustness of R&D network under cascading propagation of risk with gray attack information

Yanlu Zhang*, Naiding Yang

Department of Management Science and Engineering, School of Management, Northwestern Polytechnical University, Xi'an, Shaanxi, China

ARTICLE INFO

Article history:
Received 25 July 2012
Received in revised form
1 March 2013
Accepted 21 March 2013
Available online 6 April 2013

Keywords:
R&D network
Robustness
Cascading propagation of risk
Gray information
Complex network
Numerical simulation

ABSTRACT

Facing the cascading propagation phenomenon of risk in R&D network and the imprecision of attack information, this paper builds the cascading propagation model of risk with gray attack information. In this model, gray attack information described by node degree is measured by negative and positive deviations, and the critical threshold of resisting risk is also proposed as a new indicator of robustness of R&D network. Then the paper analyzes the robustness of R&D network under cascading propagation of risk with gray attack information through numerical simulation. The results show that R&D network has the strongest robustness under random attack, but has the weakest one under intentional attack; robustness of R&D network increases with the increase of deviation from attack information, which becomes increasingly significant when all enterprises' capacities distribution is heterogeneous; robustness of R&D network under one attack decreases with the increasing heterogeneity of all enterprises' capacities distribution; robustness of R&D network is more sensitive to the negative deviation than to the positive deviation from attack information. This research work will provide a theoretical basis for preventing and controlling cascading propagation in R&D network in the future.

1. Introduction

In recent years, R&D network is becoming an effective organizational form from which a number of enterprises could gain their competitive edges. As a new pattern of R&D collaboration, R&D network is able to break the limitations of geography and time, and satisfy enterprises' needs for affluent resources, shortened cycle time and reduced cost [1]. Nevertheless, some risks still exist in R&D network, such as market risk, collaboration risk, ethical risk and so on [2]. Moreover, risks in R&D network are interrelated due to complicated relationships among enterprises. A few risks on failed enterprises may trigger some other potential risks on neighboring enterprises just like reaction chains or amplification chains [3]. Consequently, this phenomenon may cause most of enterprises to fail and the whole R&D network to collapse, which is called cascading propagation of risk in this paper. Therefore, how to improve the robustness [4] or flexibility [5] of R&D network has become an important issue. So, it is very essential and meaningful to explore robustness of R&D network under cascading propagation of risk.

The earlier research work about robustness of complex network has always been studied by many researchers. Albert explored robustness of complex network under two types of attacks, one is random attack that the nodes are attacked randomly, the other one is intentional attack that the nodes with high-degree are attacked preferentially. He also found that scale-free network has the strongest robustness under random attack, but has the greatest vulnerability under intentional attack [4]. Subsequently, some other scholars also made many valuable findings based on Albert's work, [6–12]. However, the research mentioned above mainly focused on connectivity robustness after removal of nodes from the viewpoint of static typological structure without taking into account the dynamic process in network [13].

Considering that, some researchers started to study the cascading failure and then analyze robust of network under this dynamic process. So far, there has been a general consensus that each node of most networks bears its dynamic load, and a few nodes' failure will lead to reallocation of other nodes' loads. If a node's load surpasses its maximum capacity, then the node will be removed from network. This phenomenon will continue and probably cause the whole network to collapse, which is called the cascading failure, like the power grid collapse in north-east USA and Canada in 2003 [14], congestion of internet [15], and transport networks jam [16,17]. Motter proposed a cascading failure model (ML model) and applied it to scale-free network and uniform network respectively. He found that attacking nodes with higher

* Correspondence to: Box 145, Changan Campus of Northwestern Polytechnical University Xi'an, 710129, P.R. China. Tel.: +86 13629291139; fax: +86 2988 492 499.
E-mail address: zhangyanlu0789@163.com (Y. Zhang).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.03.009

Nomeclature

d_i	degree of node i, i.e., the number of links directly connected to node i
$\tilde{d}_i$	observed degree of node i
$d_{\max}$	maximum degree of nodes in R&D network
$d_{\min}$	minimum degree of nodes in R&D network
$\langle k \rangle$	average degree of R&D network
l_λ	negative deviation from attack information
l_μ	positive deviation from attack information
m	number of existing nodes connected to a new node at each time step
m_0	number of nodes in an original R&D network
n_k	number of nodes with the degree k
p_i	occurrence probability of risk R_i
$s_i(t)$	variable that indicates whether enterprise i functions well or not at time t
$visit(i)$	variable that indicates whether failed node i has been removed from network or not
w_j	impact created by risk R_j
$A=[a_{ij}]_{N\times N}$	adjacency matrix of R&D network with N nodes
C_i	capacity of resisting risk for node i
$G(V,E)$	R&D network with $V=\{1,2,\ldots,N\}$ and $E=\{e_{ij}\|i,j\in V\}$
$H=[h_{ij}]_{7\times 7}$	risk triggering probability matrix of R&D network
$I(t)$	proportion of failed enterprises in R&D network at the end of time t
I^*	ultimate value when cascading propagation of risk comes to an end
$L_i(t)$	sum of impacts created by risks that have occurred on enterprise i at time t
$P(k)$	degree distribution of all nodes in R&D network
R_1	market risk in R&D network
R_2	economic risk in R&D network
R_3	policy environment risk in R&D network
R_4	ethical risk in R&D network
R_5	time risk in R&D network
R_6	capital risk in R&D network
R_7	collaboration risk in R&D network
$\overline{V}$	average impact created by all risks in R&D network
$Z_j(t)$	set of neighboring failed nodes that have not been removed from network of node j at the end of time t
α	parameter that controls the distribution of all enterprises' capacities of resisting risk
β	parameter that is called the allowable threshold of resisting risk of R&D network
β^*	critical threshold of resisting risk of R&D network
λ	parameter that governs degree of negative deviation from attack information
μ	parameter that governs degree of positive deviation from attack information
δ	random variable following uniform distribution on interval [0,1]
$\eta_j^i(t)$	variable that indicates whether risk R_j on enterprise i has occurred or not at time t
$\varphi_k^{ij}(t+1)$	variable that indicates when potential risk R_k on enterprise j is triggered by the risks that have occurred on enterprise i at time t+1 or not
$\Psi_j(t)$	set of risks that have occurred on enterprise j at time t
Γ_j	set of neighboring nodes of node i
Π_i	probability that a new node links to an existed node i in the network

loads will lead to cascading failure more probably and decrease network efficiency faster for scale-free network, but uniform network still has strong robustness under both random attack and intentional attack [18]. Crucitti proposed that the more heterogeneous the distribution of all nodes' loads is, the broader the range of cascading failure in network [19]. Wu [20] and Xia [21] further used different networks to validate the conclusions made by Motter and Crucitti. Schafer [22], Zhao [23], Yang [24], and Wang [25] also proposed that it is an effective way to protect the nodes with higher degrees or make distribution of nodes' loads relatively uniform for preventing cascading failure. Wang explored robustness of power grid in western America under high-degree attack and low-degree attack through numerical simulation [26]. After that, many researchers extensively studied on the influence of attack strategies [27,28], prevention and control of cascading failure [29,30], optimization under cascading failure [31], etc., and also made many valuable findings.

Based on the research work mentioned above, we find that earlier research mainly focuses on robustness of network under random attack and intentional attack. In fact, this two kinds of attacks are just two extremes in real-world networks. From the perspective of information, the so-called random attack and intentional attack correspond to dark information (i.e., absolutely imprecise information) and white information (i.e., absolutely precise information) [32]. In many cases, most of obtained information is imprecise information between them. In other words, one can observe the degrees of all nodes, but the obtained information may be imprecise, which is called gray information in this paper. Although Gallos [33,34], Wu [35,36], and Li [37] explored connectivity robustness of network with gray attack information, they did not concern the dynamic propagation process in network, i.e., the called cascading propagation of risk in R&D network. For these two reasons, two parameters that govern the degree of positive deviation and negative deviation from real attack information are introduced into the cascading propagation model of risk in R&D network. Then robustness of R&D network under cascading propagation of risk with different imprecision of gray attack information is analyzed through numerical simulation. Our research work will provide a theoretical basis for preventing and controlling cascading propagation of risk in R&D network.

2. Modeling the cascading propagation of risk with gray information

2.1. Basic concepts

We hypothesize that R&D network is modeled as a complex network with nodes (i.e., enterprises), and edges between nodes (i.e., relationships between enterprises). Based on this, we use an undirected graph $G(V, E)$ to describe R&D network, where $V=\{1, 2, \ldots, N\}$ is the set of nodes, and $E=\{e_{ij}|i,j\in V\}$ is the set of edges. Define the adjacency matrix of R&D network with $A=[a_{ij}]_{N\times N}$, where $a_{ij}=1$ if nodes i and j are connected directly and $a_{ij}=0$ if there is no direct connection between nodes i and j. Let $d_i(1\le i\le N)$ be the degree of node i, which is the number of nodes connecting directly with node i, and let $d_{\min}$ be the minimum node degree and $d_{\max}$ be the maximum node degree in R&D network, apparently we have $d_{\min}\le d_i\le d_{\max}(\forall i\in V)$. Let $P(k)$ be the degree distribution of all nodes in R&D network, which can be calculated by the